NETGEAR

N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

June 2013
202-10941-03
v1.0

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Contents

Chapter 1 Hardware Setup

Unpack Your Modem Router 9
Hardware Features 10
Front Panel 10
Back Panel 12
Label 13
Position Your Modem Router 13
ADSL Microfilters 14
One-Line ADSL Microfilter (Not Included) 14
Two-Line ADSL Microfilter (Included) 14
Summary 15
Cable Your Modem Router 15
Verify the Cabling 16

Chapter 2 Access the Modem Router

Modem Router Setup Preparation 18
Use Standard TCP/IP Properties for DHCP 18
Replace an Existing Router 18
Adapters and Security Settings 18
Gather ISP Information 18
Wireless Devices and Security Settings 19
Types of Logins and Access 19
NETGEAR genie Setup 19
Use NETGEAR genie after Installation 21
Upgrade the Firmware 21
Dashboard (BASIC Home Screen) 22
Join Your Wireless Network 23
Manual Method 23
Wi-Fi Protected Setup (WPS) Method 23
NETGEAR genie App and Mobile genie App 24

Chapter 3 NETGEAR genie Basic Settings

Internet Setup 26
Internet Setup Screen Fields 27
Basic Wireless Setup 30
Wireless Setup Screen Fields 32
Change the WEP Security Option 33
Change the WPA Security Option and Passphrase 34
View Attached Devices 35

Parental Controls 36
Set Up a Guest Network. 39

Chapter 4 NETGEAR genie Advanced Home

NETGEAR genie Advanced Home Screen 41
Setup Wizard 41
WPS Wizard 42
ADSL Setup 43
WAN Setup. 45
WAN Setup Screen Fields 46
Default DMZ Server 47
Change the MTU Size 48
LAN Setup 49
LAN Setup Screen Settings 51
Specify DHCP Server Settings 51
Address Reservation 52
Quality of Service (QoS) Setup 53
WMM QoS for Wireless Multimedia Applications 53
Set Up QoS for Internet Access 53

Chapter 5 USB Storage

USB Drive Requirements 59
Connect a USB Storage Device to the Modem Router 59
Access the USB Storage Device 60
File-Sharing Scenarios 61
Share Photos 62
Store Files in a Central Location for Printing 62
Share Large Files over the Internet 62
View a USB Device Attached to the Modem Router 63
USB Storage Device Network and Access Settings. 63
Available Network Folders 64
Media Server Settings 66
Specify Approved USB Devices 67
Connect to the USB Drive from a Remote Computer. 68
Connect to the USB Drive with Microsoft Network Settings 68
Enable File and Printer Sharing 69
Configure Windows 98SE and Windows ME 69
Configure Windows 7, Windows XP, Windows 2000 69
Safely Remove a USB Drive 69

Chapter 6 Security

Keyword Blocking of HTTP Traffic 71
Block Services (Port Filtering) 72
Set Up Firewall Rules to Control Network Access 73
Remote Computer Access Basics 73
Port Triggering to Open Incoming Ports 75

Port Forwarding to Permit External Host Communications 76
How Port Forwarding Differs from Port Triggering 77
Set Up Port Forwarding to Local Servers 77
Set Up Port Triggering 79
Schedule When to Block the Internet 82
Security Event Email Notifications 82

Chapter 7 Administration

Update the Modem Router Firmware 85
View Router Status 86
Router Information 86
Internet Port 87
Wireless Settings (2.4 GHz) 89
View Logs of Web Access or Attempted Web Access 90
Manage the Configuration File 92
Back Up Settings 92
Restore Configuration Settings 92
Erase the Current Configuration Settings 93
Change the Password 93

Chapter 8 Advanced Settings

Advanced Wireless Settings 95
Control the Wireless Radio 95
View or Change WPS Settings 96
Set Up a Wireless Access List by MAC Address 96
Wireless Distribution System (WDS) 98
Set Up the Base Station 99
Set Up a Repeater 100
Set Up a Point-to-Point Bridge 102
Set Up a Multi-Point Bridge 103
Repeater with Wireless Client Association 105
Dynamic DNS 106
Static Routes 107
Remote Management 109
Universal Plug and Play 111
IPv6 112
Requirements for Entering IPv6 Addresses 112
Auto Detect 113
IPv6 6to4 Tunnel 114
IPv6 Pass Through 115
IPv6 Fixed 115
IPv6 DHCP 117
IPv6 PPPoE 118
Traffic Meter 119

Chapter 9 Virtual Private Networking

Overview of VPN Configuration 123
Client-to-Gateway VPN Tunnels. 123
Gateway-to-Gateway VPN Tunnels 123
Set Up a Client-to-Gateway VPN 124
Add a Gateway-to-Gateway VPN Tunnel. 125
Activate a VPN Tunnel 128
View or Change the Status of a VPN Tunnel 128
Deactivate a VPN Tunnel 130
Delete a VPN Tunnel 131
Auto Policy Example 131
Add or Edit a VPN Auto Policy 131
Add or Edit a Manual VPN Policy. 135

Chapter 10 Troubleshooting

Troubleshoot with the LEDs 140
Power LED Is Off 140
Power LED Is Red 140
LAN LED Is Off. 140
Wireless LEDs Are Off 141
DSL or Internet LED Is Off 141
Cannot Log In to the Modem Router 141
Troubleshoot the Internet Connection 142
ADSL Link. 142
Internet LED Is Red 143
Obtaining an Internet IP Address 143
Troubleshoot PPPoE or PPPoA. 144
Troubleshoot Internet Browsing 144
TCP/IP Network Not Responding. 144
Test the LAN Path to Your Modem Router. 145
Test the Path from Your Computer to a Remote Device 145
Cannot Log In. 146
Changes Not Saved 147
Incorrect Date or Time 147

Appendix A Supplemental Information

Factory Settings 149
Specifications 151

Appendix B VPN Configuration

Configuration Profile. 153
Step-by-Step Configuration 153
Modem Router with FQDN to Gateway B 154
Configuration Profile. 154
Step-by-Step Configuration 156

Configuration Summary (Telecommuter Example) 158
Set Up Client-to-Gateway VPN (Telecommuter Example) 159
Configure Gateway A (VPN Router at Main Office) 159
Configure Gateway B (VPN Router at Regional Office) 160
Monitor the VPN Tunnel (Telecommuter Example) 167

Appendix C Notification of Compliance

Hardware Setup

1

The NETGEAR N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B offers dual-band technology and ensures top speeds and the greatest range for demanding applications, such as streaming HD video and multiplayer gaming. Complete with a built-in ADSL modem, it is compatible with all major ADSL Internet service providers. The gigabit port on the WAN side has an option to connect to a fiber/cable modem.

The modem router supports the following NETGEAR green features:

- Power On/Off button
- 80% recycled packaging
- CEC (California Efficiency)
- RoHS
- WEEE

If you have not already set up your new modem router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Access the Modem Router*, explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Modem Router*
- *Hardware Features*
- *Position Your Modem Router*
- *ADSL Microfilters*
- *Cable Your Modem Router*
- *Verify the Cabling*

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

If you want instructions about how to wall-mount your modem router, see Wall-Mount Your Router at *http://support.netgear.com/app/answers/detail/a_id/18725*.

Unpack Your Modem Router

Your box contains the following items:

- N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Installation guide with cabling and router setup instructions.

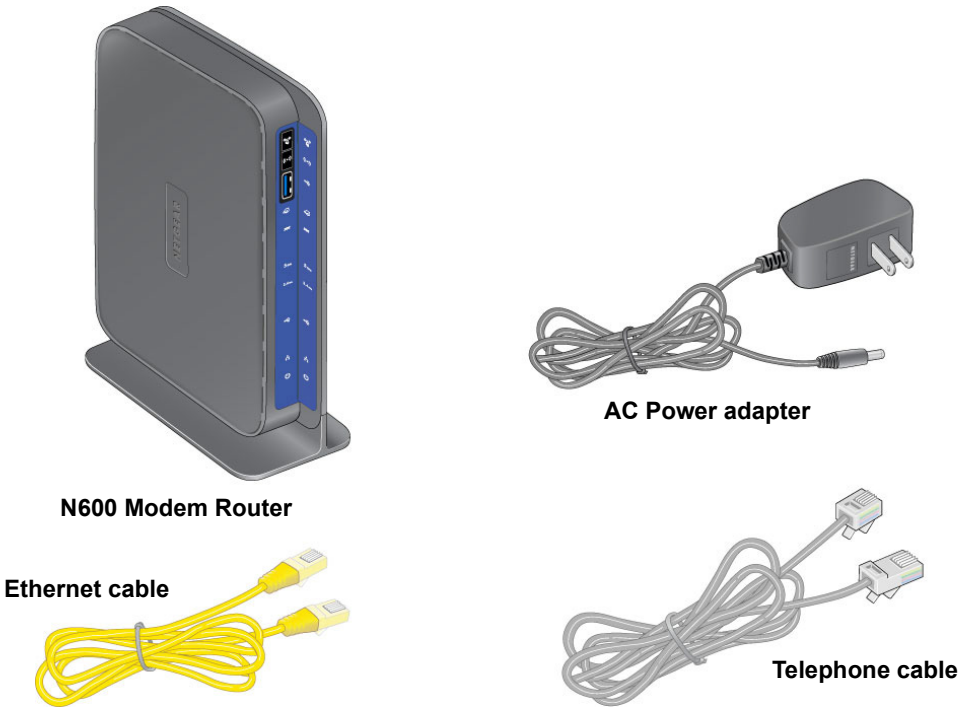


Figure 1. Package contents

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials in case you need to return the product for repair.

Hardware Features

Before you cable your modem router, take a moment to become familiar with the front panel, back panel, and label. Pay particular attention to the LEDs on the front panel.

Front Panel

The modem router front panel has the status LEDs and icons shown in the figure. The WiFi and WPS icons are buttons.

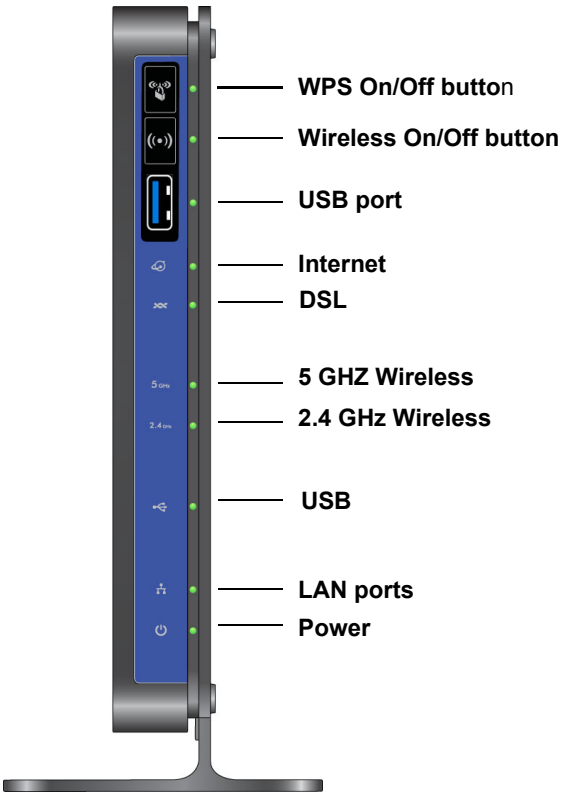


Figure 2. Front panel LEDs and icons

Front Panel Buttons and USB Port

WPS button. You can use this button to add a wireless computer or device to your network using Wi-Fi Protected Setup. The wireless computer or device has to support WPS. For more information, see *Wi-Fi Protected Setup (WPS) Method* on page 23.

Wireless On/Off button. This button turns the wireless radio of the modem router off and on. For more information, see *Advanced Wireless Settings* on page 95.

USB port. You can use this port to connect USB storage devices like flash drives or hard drives.

Front Panel LEDs

The following table describe the LEDs on the front panel from top to bottom.

Table 1. LED descriptions

LED	Description
Internet	• **Solid green**. You have an Internet connection. If this connection is dropped due to an idle time-out but the connection is still present, the light stays green. If the Internet connection is dropped for any other reason, the light turns off. • **Solid red**. The Internet (IP) connection failed. For more information about troubleshooting the internet connection, see *Troubleshoot the Internet Connection* on page 142. • **Blinking green**. Data is being transmitted over the Internet connection. • **Off**. No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).
DSL	• **Solid green**. You have an ADSL connection. In technical terms, the ADSL port is synchronized with an ISP's network-access device. • **Blinking green**. Indicates that the modem router is negotiating the best possible speed on the ADSL line. • **Off**. The unit is off or there is no IP connection.
5 GHz Wireless	• **Solid blue**. There is wireless connectivity. • **Blinking blue**. Data is being sent or received over the 5 GHz wireless link. • **Off**. There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.
2.54 GHz Wireless	• **Solid green**. There is wireless connectivity. • **Blinking green**. Data is being sent or received over the 2.4 GHz wireless link. • **Off**. There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.
USB	• **Solid green**. A USB port has detected a USB device. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on these ports.
LAN (Ethernet)	• **Solid green**. A LAN port has detected an Ethernet link with a device. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on these ports.
Power	• **Solid green**. Power is supplied to the modem router. • **Solid red**. POST (power-on self-test) failure or a device malfunction has occurred. • **Off**. Power is not supplied to the modem router. • **Restore Factory Settings**. The Power LED blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for 6 seconds. The Power LED blinks red three times when the Restore Factory Settings button is released and then turns green as the modem router resets to its factory defaults.

Back Panel

The back panel has the buttons and port connections as shown in the following figure.

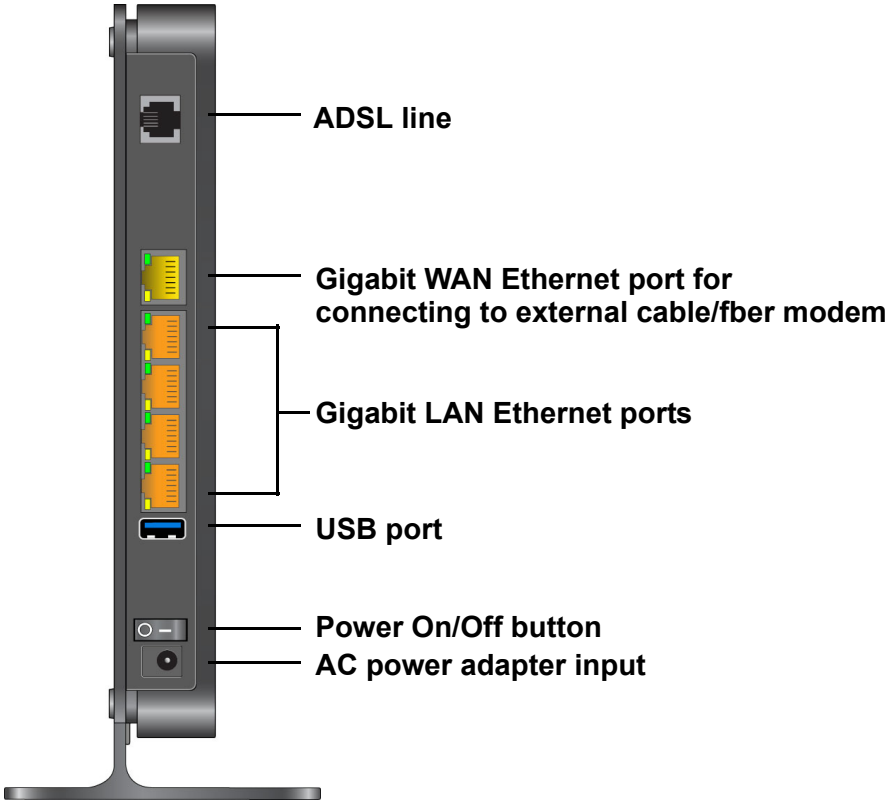


Figure 3. Back panel connections and buttons

For information about resetting the modem router to its factory settings, see *Factory Settings* on page 149.

Label

The label on the bottom of the modem router shows the router's Restore Factory Settings button, serial number, MAC address, Wi-Fi network name (SSID), and network key (password).

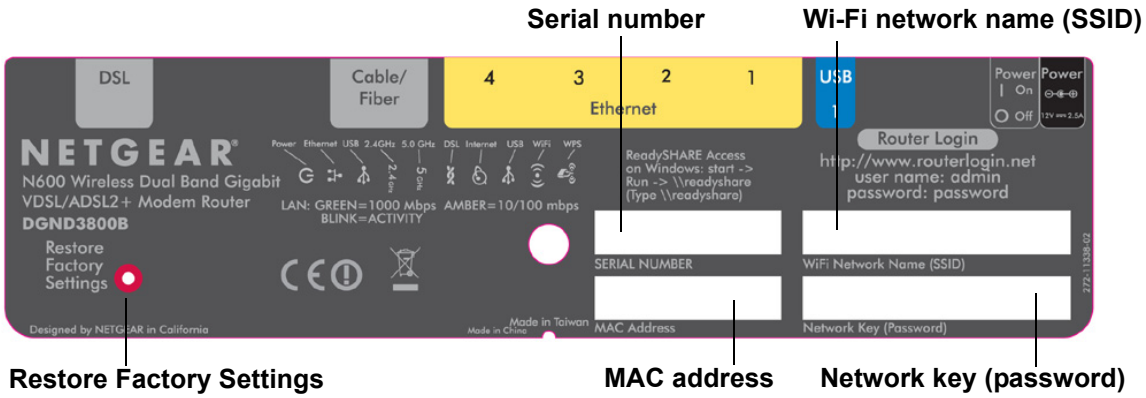


Figure 4. Label on modem router bottom

Position Your Modem Router

The modem router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem router:

- Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or a 2.4 GHz cordless phone and its base.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

ADSL Microfilters

If this is the first time you have cabled a modem router between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your Modem Router* on page 15.

An ADSL microfilter is a small inline device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service needs an ADSL microfilter to filter out the DSL interference. Examples of devices are telephones, fax machines, answering machines, and caller ID displays. Not every phone line in your home necessarily carries DSL service. That depends on the DSL service setup in your home.

Note: Often the ADSL microfilter is in the box with the modem router. If you purchased the modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter (Not Included)

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The modem router plugs directly into a separate DSL line. Plugging the modem router into the phone jack blocks the Internet connection. If you do not have a separate DSL line for the modem router, the best thing to do is to use an ADSL microfilter with a built-in splitter (see *Two-Line ADSL Microfilter (Included)* on page 14).

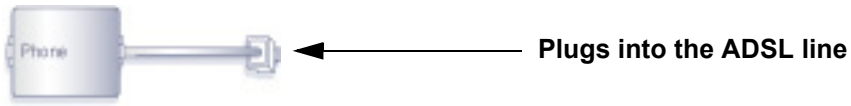


Figure 5. One-line ADSL microfilter

To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

Two-Line ADSL Microfilter (Included)

Use an ADSL microfilter with a built-in splitter if you have a single wall outlet that provides connectivity for both the modem router and your telephone equipment. Plug the ADSL

microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the modem router into the jack labeled ADSL.

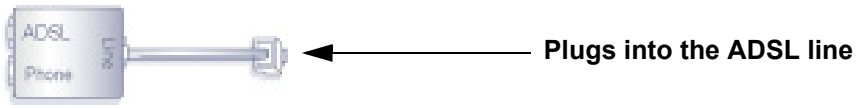


Figure 6. Two-line ADSL microfilter with built-in splitter

Summary

- **One-line ADSL microfilter (not included)**. Use with a phone or fax machine.
- **Splitter (not included)**. Use with a one-line ADSL microfilter to share an outlet with a phone and the modem router.
- **Two-line ADSL microfilter with built-in splitter (included)**. Use to share an outlet with a phone and the modem router.

Cable Your Modem Router

You can use either a DSL or a cable/fiber Internet connection.

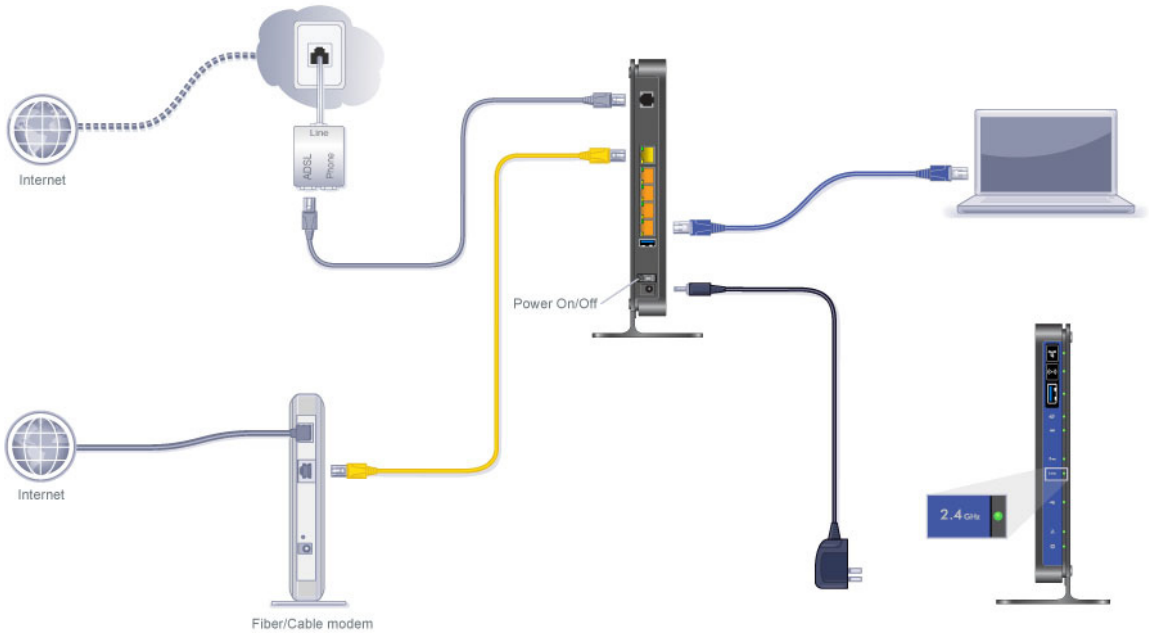


Figure 7. Cable connections

CAUTION:

Incorrectly connecting a filter to your modem router blocks your DSL connection.

For help with installation, see the installation guide that came in the package with your product.

For information about how to access the modem router to view or change the settings, see *Chapter 2, Access the Modem Router*.

Verify the Cabling

Verify that your router is cabled correctly by checking the modem router LEDs. Turn on the modem router by pressing the **Power On/Off** button on the back.

- The Power LED is green when the modem router is turned on.
- The LAN port is green when a computer is cabled to the router by an Ethernet cable.
- The Wireless LEDs are lit when the modem router is turned on.
- The DSL LED is green when you have an ADSL connection.
- The Internet LED is red when there is no Internet connection.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically.

2 Access the Modem Router

This chapter explains how to use NETGEAR genie to set up your modem router after you complete cabling as described in the installation guide and in the previous chapter.

This chapter contains the following sections:

- *Modem Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade the Firmware*
- *Dashboard (BASIC Home Screen)*
- *Join Your Wireless Network*
- *NETGEAR genie App and Mobile genie App*

Modem Router Setup Preparation

You can set up your modem router with the NETGEAR genie automatically, or you can use the genie menus and screens to set up your modem router manually. Before you start the setup process, get your ISP information and make sure the computers and devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you need to change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Replace an Existing Router

To replace an existing router, disconnect it completely from your network and set it aside before starting the router setup.

Adapters and Security Settings

A wireless adapter is the wireless radio in your computer that lets the computer connect to a wireless network. Most computers come with an adapter already installed, but if it is outdated or slow, you can purchase a USB adapter to plug into a USB port.

Make sure the wireless adapter in each computer in your wireless network supports the same security settings as the modem router.

Note: If you connect devices to your modem router using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 33, those devices assume the security settings of the router.

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in. Make sure that you have the following information:

- Active Internet service provided by an ADSL account
- The ISP configuration information for your DSL account
  - ISP login name and password

- ISP Domain Name Server (DNS) addresses
- Fixed or static IP address
- Host and domain names
- Depending on how your ISP set up your Internet account, you could need to know one or more of there settings for a manual setup:
  - Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters
  - Multiplexing method
  - Host and domain names

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the modem router.

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Modem router login** logs you in to the modem router interface. For more information about this login, see *Use NETGEAR genie after Installation* on page 21.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your modem router.

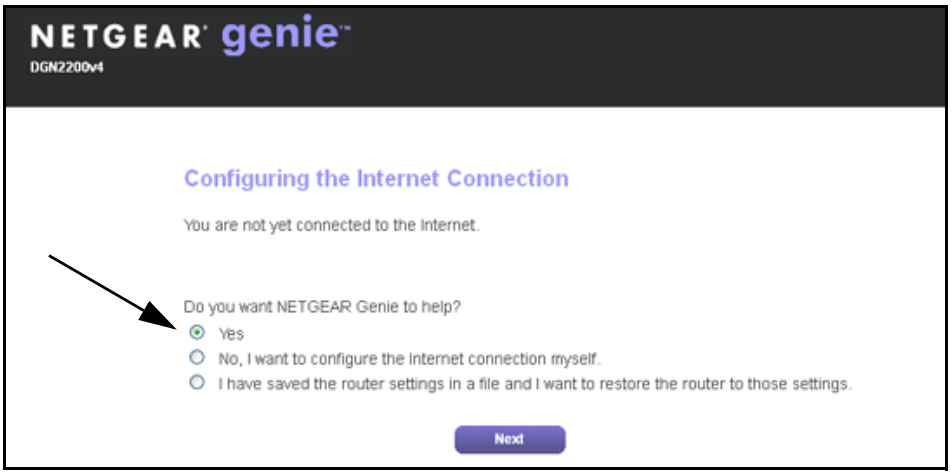
NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. Installation and basic setup takes about 15 minutes to complete.

➢ **To use NETGEAR genie to set up your modem router:**

1. Turn on the modem router by pressing the **On/Off** button.
2. Make sure that your computer or wireless device is connected to the modem router with an Ethernet cable (wired) or wirelessly with the preset security settings listed on the bottom label.
3. Launch your Internet browser.

- The first time you set up the Internet connection for your modem router, the browser goes to http://www.routerlogin.net, and the NETGEAR genie screen displays.



- If you already used the NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie after Installation* on page 21.

4. Follow the onscreen instructions to complete NETGEAR genie setup.

   NETGEAR genie guides you through connecting the modem router to the Internet.

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports or wirelessly to the modem router.
- Make sure that the modem router has full power, and that its WiFi LED is lit.
- To make sure that the browser does not cache the previous page, close and reopen the browser.
- Browse to **http://www.routerlogin.net**.
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the modem router.

If the modem router does not connect to the Internet:

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 10, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

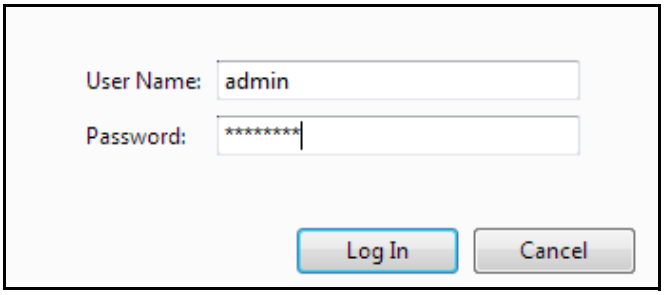
Use NETGEAR genie after Installation

When you first set up your modem router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the modem router. If you want to view or change settings for the modem router, you can use genie again.

➢ **To use NETGEAR genie again after installation:**

1. Launch your browser from a computer or wireless device that is connected to the modem router.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

   The login window displays:



3. Enter **admin** for the modem router user name and **password** for the modem router password, both in lowercase letters.

   Note: *The modem router user name and password are different from the user name and password for logging in to your Internet connection. For more information, see Types of Logins and Access on page 19.*

Upgrade the Firmware

When you set up your modem router and are connected to the Internet, the modem router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. For more information, see *Update the Modem Router Firmware* on page 89.

Click the message when it shows up, and click **Yes** to upgrade the modem router with the latest firmware. After the upgrade, the modem router restarts.

CAUTION:

Do not try to go online, turn off the modem router, shut down the computer, or do anything else to the modem router until the modem router finishes restarting and the Power LED has stopped blinking for several seconds.

Dashboard (BASIC Home Screen)

The modem router BASIC Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view and change the settings. The left column has menus. You can use the ADVANCED tab to access more menus and screens.

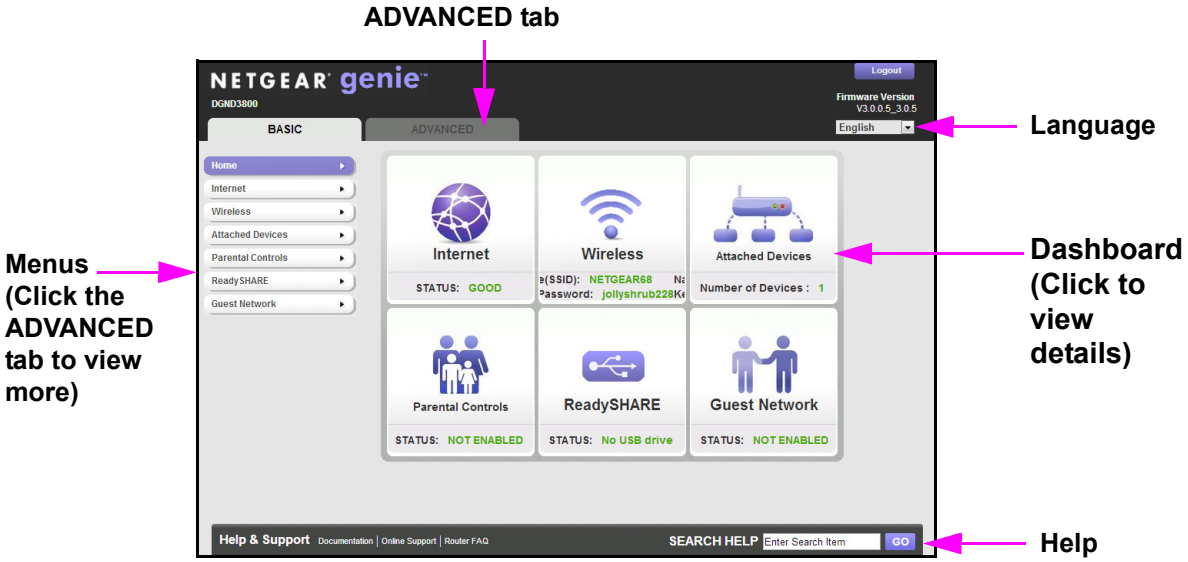


Figure 8. BASIC Home screen with dashboard, language, and online help

- **Home**. This dashboard screen displays when you log in to the modem router**.**
- **Internet**. Set, update, and check the ISP settings of your modem router.
- **Wireless**. View or change the wireless settings for your modem router.
- **Attached Devices**. View the devices connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.
- **ReadySHARE**. If you connected a USB storage device to the modem router, then it is displayed here.
- **Guest Network**. Set up a guest network to allow visitors to use your modem router's Internet connection.
- **ADVANCED tab**. Set the modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 8, Advanced Settings*. You need a solid understanding of networking to use this tab.
- **Help & Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Join Your Wireless Network

You can use the manual or the WPS method to join your wireless network. For instructions about how to set up a guest network, see *Set Up a Guest Network* on page 39.

Manual Method

With the manual method, choose the network that you want and type its password to connect.

➢ **To connect manually:**

1. On your computer or wireless device, open the software that manages your wireless connections. This software scans for all wireless networks in your area.
2. Look for your network and select it.

   The unique WiFi network name (SSID) and password are on the modem router label. If you changed these settings, look for the network name that you used.
3. Enter the modem router password and click **Connect**.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, press a button or enter a PIN. NETGEAR calls WPS Push 'N' Connect.

Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2 or WPA wireless security.

➢ **To use WPS to join the wireless network:**

1. Press the **WPS** button on the modem router front panel .
2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device.

   The WPS process automatically sets up your wireless computer with the network password and connects you to the wireless network.
3. Repeat steps 1–2 to add other WPS wireless devices.

NETGEAR genie App and Mobile genie App

The genie app is the easy dashboard for managing, monitoring, and repairing your home network. See the *NETGEAR genie App User Manual* for details about the genie apps.

Figure 9. genie app dashboard

The genie app can help you with the following:

- Automatically repair common wireless network problems.
- Have easy access to features like Live Parental Controls, guest access, Internet traffic meter, speed test, and more.

The genie mobile app works on your iPhone, iPad, or Android phone:

Figure 10. genie mobile app home screen

NETGEAR genie Basic Settings

3

This chapter contains the following sections:

- *Internet Setup*
- *Basic Wireless Setup*
- *View Attached Devices*
- *Parental Controls*
- *Set Up a Guest Network*

For information about ReadySHARE USB storage, see *Chapter 5, USB Storage*.

Internet Setup

The Internet Setup screen is where you view or change basic ISP information.

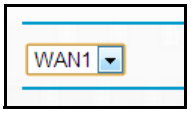
Note: You can use the Setup Wizard to detect the Internet connection and automatically set up the modem router. See *Setup Wizard* on page 41.

➤ **To view or change the basic Internet setup:**

1. From the Home screen, select **Internet**.

The fields that display in the Internet Setup screen depend on whether your Internet connection requires a login.

2. From the WAN connection drop down menu, select **WAN1**.



- If the DSL port is plugged in, WAN1 is configured for DSL.
- If the WAN Ethernet port is plugged in, WAN1 is configured for Ethernet.
- If both the DSL port and WAN Ethernet port have been plugged in, only the DSL port is active and the WAN Ethernet port is disabled because only one WAN port can be active.

Note: WAN1 is for normal Internet access and WAN2 is for IPTV service. If you are subscribed to IPTV, you need to set up WAN2. The set up for WAN1 and WAN2 should be the same. If you are not subscribed to IPTV service, you do not need to set up WAN2. VLAN tags are used to distinguish the WAN1 and WAN2 traffic.

3. Select one of the following radio buttons, and fill in the fields:
   - **Yes**. Select the encapsulation method and your internet service provider.
   - **No**. Enter the account and domain names, only if needed.
4. Enter the settings for the IP address and DNS server.

   The default settings usually work fine. If you have problems with your connection, check the ISP settings.
5. Click **Apply** to save your settings.
6. Click **Test** to test your Internet connection.

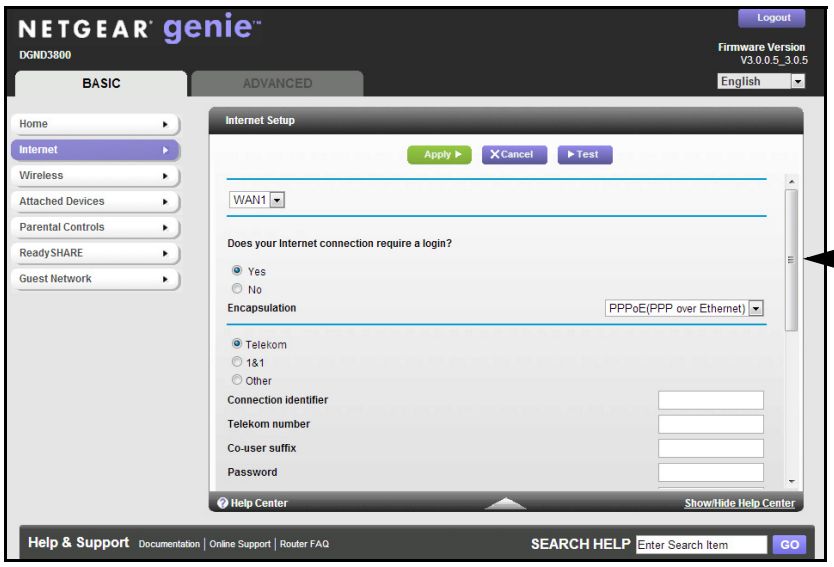
   If the NETGEAR website does not display within 1 minute, see *Chapter 10, Troubleshooting*.

Internet Setup Screen Fields

The following descriptions explain all of the possible fields in the Internet Setup screen. The fields that display in this screen depend on whether tan ISP login is required.

Does Your Internet connection require a login? Answer either yes or no.

If your ISP requires a login and you selected yes, the following screen displays:



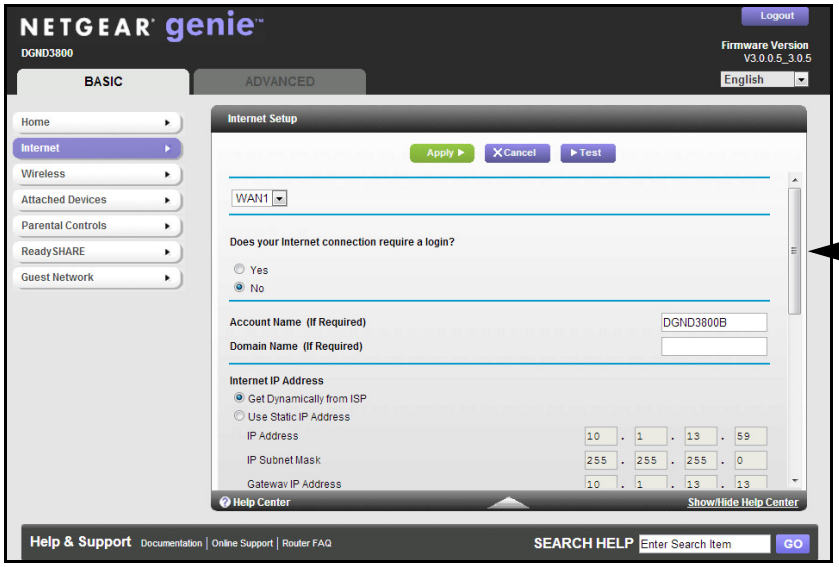
Scroll to view more settings

These fields display when your ISP requires a login:

- **Encapsulation**. Encapsulation is a method for enclosing multiple protocols. PPP stands for Point-to-Point Protocol. The choices are PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM).
- **Telekom**. Select the **Telekom** radio button if Telekom is your ISP. The following fields display:
  - **Connection identifier**. The connection identifier provided by Telekom.
  - **Telekom number**. The Telekom number provided by Telekom.
  - **Co-user suffix**. The co-user suffix provided by Telekom.
  - **Password**. The password that you use to log in to Telekom.
  - **Service Name (If Required)**. If Telekom provided a service name, enter it here.
  - **Idle Timeout (In Minutes)**. If you want to change the login time-out, enter a new value in minutes. This setting determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. A value of 0 (zero) means never log out.
- **1&1**. Select the 1&1 radio button if **1&1** is your ISP. The following fields display:
  - **Login**. The login name provided 1&1. This login name is often an email address.
  - **Password**. The password that you use to log in to 1&1.
  - **Service Name (if Required)**. If 1&1 provided a service name, enter it here.
  - **Idle Timeout (In minutes)**. If you want to change the login time-out, enter a new value in minutes. This setting determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. A value of 0 (zero) means never log out.
- **Other**. Select the Other radio button if your ISP is not displayed. The following fields display:
  - **Login**. The login name provided by your ISP. This login name is often an email address.
  - **Password**. The password that you use to log in to your ISP.
  - **Service Name (if Required)**. If your ISP provided a service name, enter it here.
  - **Idle Timeout (In minutes)**. If you want to change the login time-out, enter a new value in minutes. This setting determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. A value of 0 (zero) means never log out.
- **Internet IP Address**.
  - **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
  - **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's modem router to which your modem router will connect.
- **Domain Name Server (DNS) Address**. The DNS server is used to look up site addresses based on their names.

  - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
  - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
- **NAT (Network Address Translation)**. NAT allows computers on your home network to share the modem router Internet connection. NAT is enabled by default because it is needed in most situations. The following settings are available:
  - Enable
  - Disable
  - Disable Firewall

If your ISP does not require a login and you selected no, the following screen displays:



Scroll to view more settings

These fields display when no login is required:

- **Account Name (If required)**. Enter the account name provided by your ISP. This might also be called the host name.
- **Domain Name (If required)**. Enter the domain name provided by your ISP.
- **Internet IP Address**.
  - **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
  - **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's modem router to which your modem router will connect.
  - **Use IP Over ATM (IPoA)**. Your ISP uses classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.
- **Domain Name Server (DNS) Address**. The DNS server is used to look up site addresses based on their names.

  - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
  - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
- **NAT (Network Address Translation)**. NAT allows computers on your home network to share the modem router Internet connection. NAT is enabled by default because it is needed in most situations. The following settings are available:
  - Enable
  - Disable
  - Disable Firewall
- **Router MAC Address**. The Ethernet MAC address that the modem router uses on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your modem router to use your computer's MAC address (also called cloning).
  - **Use Default Address**. Use the default MAC address.
  - **Use Computer MAC Address**. The modem router captures and uses the MAC address of the computer that you are now using. You have to use the one computer that the ISP allows.
  - **Use This MAC Address**. Enter the MAC address that you want to use.

Basic Wireless Setup

The Wireless Setup screen lets you view or configure the wireless network setup.

The modem router comes with preset security. This means that the Wi-Fi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the bottom of the unit.

Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

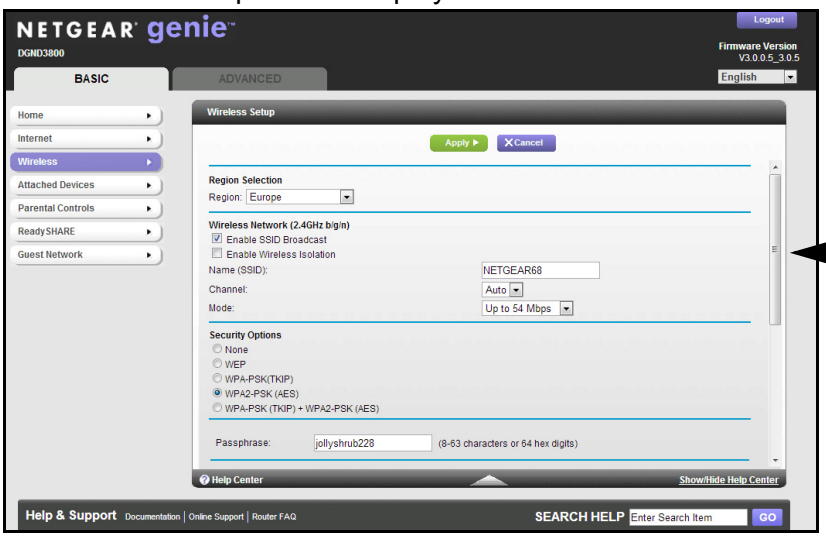
NETGEAR recommends that you do not change your preset security settings. If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

If you use a wireless computer to change the wireless network name (SSID) or other wireless security settings, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the modem router.

➢ To view or change the basic wireless setup:

1. Select **BASIC > Wireless**.

   The Wireless Setup screen displays:



Scroll to view more settings

   The screen sections, settings, and procedures are explained in the following sections.

2. Make any changes that are needed.
3. Click **Apply.**

   Your settings are saved.

   If you were connected wirelessly to the modem router and you changed the SSID or wireless security, you are disconnected from the network.

4. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:
   - Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
   - Does your wireless device or computer show up on the Attached Devices screen? If it does, it is connected to the network.
   - If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your modem router.

Wireless Setup Screen Fields

You can use this screen to view or change the wireless network settings and the security option.

Wireless Network

Region. The location where the modem router is used. Select from the countries in the list. In the United States, the region is fixed to United States and is not changeable.

Enable SSID Broadcast. This setting allows the modem router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear this check box, and click **Apply**.

Enable Wireless Isolation. If this check box is selected, computers or wireless devices that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and *NETGEAR strongly recommends that you do not change this setting.*

Channel. This setting is the wireless channel the gateway uses. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

When you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

Mode. Up to 145 Mbps is the default setting, which allows 802.11n and 802.11g wireless devices to join the network. The other settings are Up to 54 Mbps, and Up to 300 Mbps.

Security Options Settings

The Security Options section of the Wireless Setup screen lets you change the security option and passphrase. ***NETGEAR recommends that you do not change these settings***. ***Do not disable security***.

For more information about how to change the security options, see the following sections:

- *Change the WEP Security Option* on page 33
- *Change the WPA Security Option and Passphrase* on page 34

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are two types of encryption: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WPA has several options including pre-shared key (PSK) encryption.

This section presents an overview of the security options and provides guidance on when to use which option.

WEP Encryption

WEP uses an old encryption method and can be easily decoded with today's powerful computers. Use this mode only when you have a very old legacy wireless client that does not support WPA-PSK. The Wi-Fi Alliance highly recommends against using WEP and plans to make it obsolete. If you do decide to use WEP, see *Change the WEP Security Option* on page 33 for the procedure.

WPA Encryption

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means that the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking.

WPA uses a passphrase for authentication and to generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and works with all wireless network interface cards, but not all wireless access points.

WPA2-PSK is stronger than WPA-PSK. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. For help with WPA settings on your wireless computer or device, see the instructions that came with your product.

Change the WEP Security Option

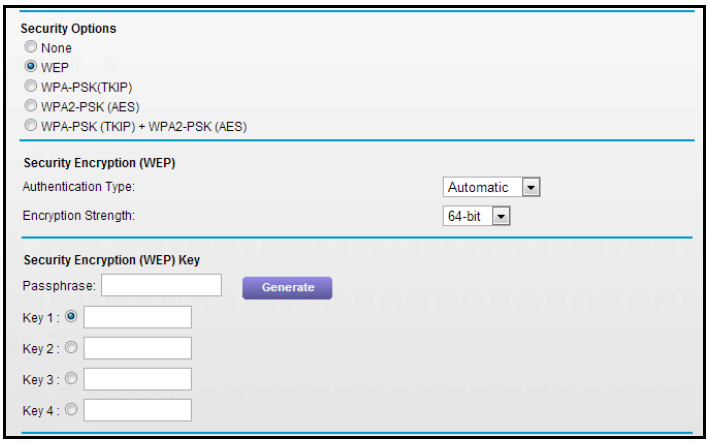
WEP is a legacy security setting. NETGEAR recommends that you use WPA2 or WPA security unless you have legacy wireless equipment that supports only WEP. WEP encryption is available only when the Mode setting is Up to 54 Mbps.

➢ **To change the WEP settings:**

1. Select **BASIC > Wireless**.

   The Wireless Setup screen displays.

2. In the Security Options section, select **WEP**:



3. Select the authentication type.

   The default is Automatic. Other choices are Open System (any client can authenticate itself to the network) and Shared Key (a passphrase and a four-way challenge is needed for authentication).

4. Select the encryption strength setting, either 64 bit or 128 bit.
5. Enter the four data encryption keys either manually or automatically.

   These values have to be identical on all computers and access points in your network.

   - **Automatic**. Enter a word or group of printable characters in the Passphrase field, and click **Generate**. The four key fields are automatically populated with key values.
   - **Manual**. The number of hexadecimal digits that you enter depends on the encryption strength setting:
     - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
     - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).

6. Select the radio button for the key you want to make active.

   Make sure that you understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the modem router.

7. Click **Save** to save your settings, or click **Apply** so your changes to take effect immediately.

Change the WPA Security Option and Passphrase

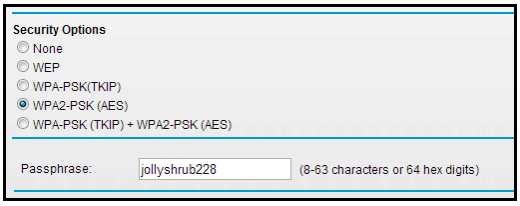
You can change the security settings for your modem router. If you do so, then write down the new settings and store them in a secure place for future reference.

➢ **To change the WPA settings:**

1. Select **BASIC > Wireless**.

The Wireless Setup screen displays.

2. Under Security Options, select the WPA option you want.



3. In the Passphrase field that displays when you select a WPA security option, enter the network key (password) that you want to use.

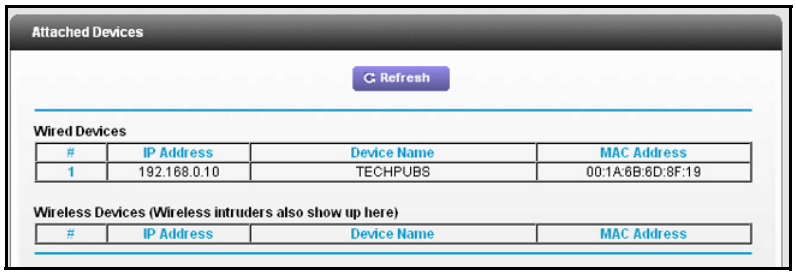
   It is a text string from 8 to 63 characters.

View Attached Devices

Use the Attached Device screen to view all computers or devices that are currently connected to your network.

➢ **To go to the Attached Devices screen:**

From the Basic Home screen, select **Attached Devices**.



Wired devices are connected to the modem router with Ethernet cables. Wireless devices have joined the wireless network.

- **# (number)**. The order in which the device joined the network.
- **IP Address**. The IP address that the modem router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
- **Device Name**. If the device name is known, it is shown here.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.

Click **Refresh** to update this screen.

Parental Controls

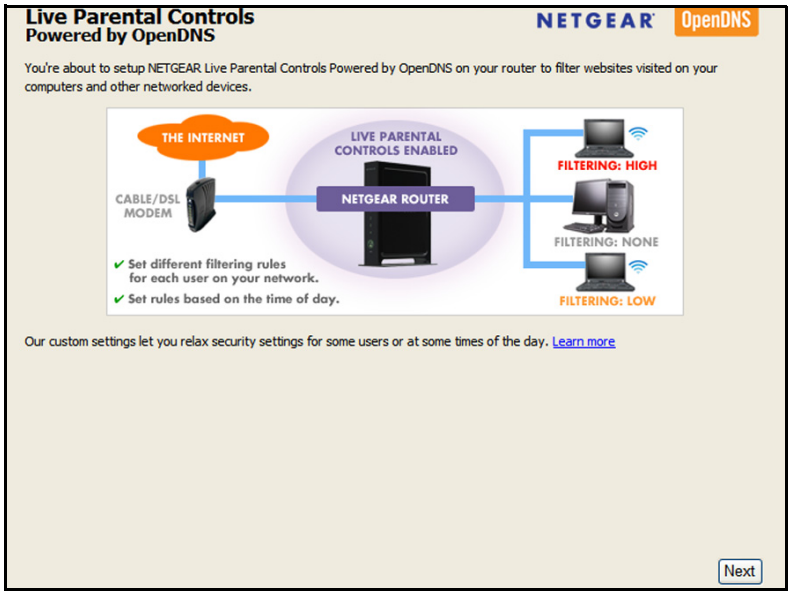
The first time you select Parental Controls from the BASIC Home screen, your browser goes to the Live Parental Controls website. You can learn more about Live Parental Controls or download the application.

Figure 11. Live Parental Controls website

➢ **To set up Live Parental Controls:**

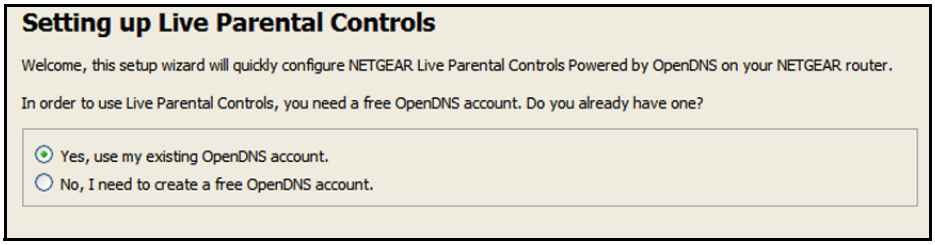
1. Select **Parental Controls** on the Dashboard screen.
2. Click either the **Windows Users** or **Mac Users** button.
3. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management Utility.

After installation, Live Parental Controls automatically starts.



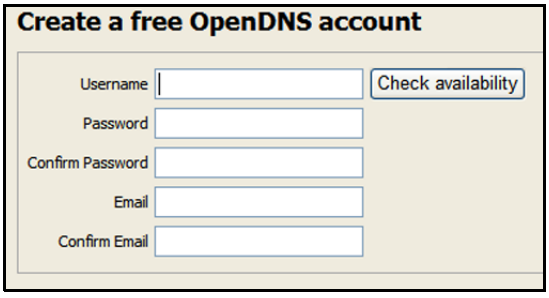
4. Click **Next**, read the note, and click **Next** again to proceed.

   Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.



5. Select the radio button that applies to you and click **Next**.
   - If you already have an OpenDNS account, leave the **Yes** radio button selected.
   - If you do not have an OpenDNS account, select the **No** radio button.

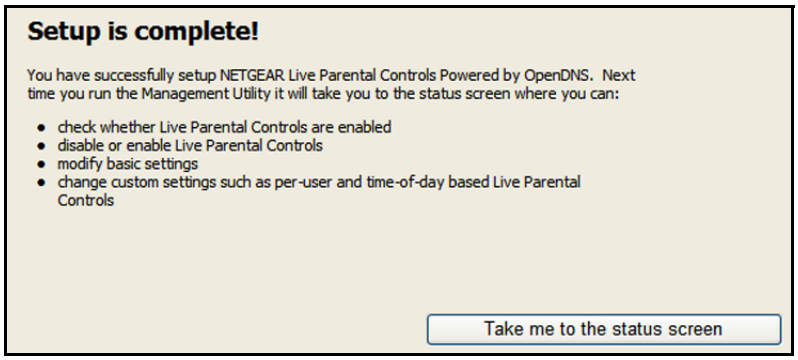
     If you are creating an account, the following screen displays:



   - Fill in the fields and click **Next**.

After you log on or create your account, the filtering level screen displays:

6. Select the radio button for the filtering level that you want and click **Next**.



7. Click the T**ake me to the status screen** button.

Parental controls are now set up for the modem router. The dashboard shows Parental Controls as Enabled.

Set Up a Guest Network

Adding a guest network allows visitors at your home to use the Internet without giving them your wireless security key.

➢ **To set up a guest network:**

1. Select **BASIC > Guest Network**.

   The Guest Network Settings page displays:

2. Select the wireless network to configure.
3. Give the guest network a name.

   The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main SSID.

4. Select any of the following wireless settings:

   Enable this wireless Network. When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.

   Enable SSID Broadcast. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.

   Allow guest to access My Local Network. If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.

   Enable Wireless Isolation. If this check box is selected, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network.

5. Select a security option from the list.

   The security options are described in *Security Options Settings* on page 32.

6. Click **Apply**.

   Your settings are saved.

NETGEAR genie Advanced Home

4

This chapter contains the following sections:

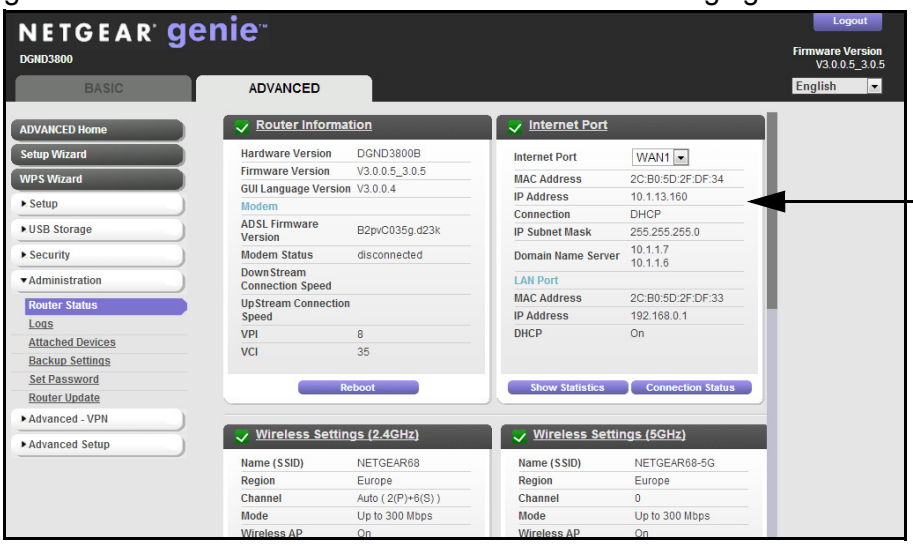
- *NETGEAR genie Advanced Home Screen*
- *Setup Wizard*
- *WPS Wizard*
- *ADSL Setup*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service (QoS) Setup*

Some selections on the Advanced screen are described in separate chapters:

- **Internet Setup**. This screen can be accessed through both the Setup menu on the Advanced screen and the dashboard on the Basic Home screen. For more information, see *Internet Setup* **on page 26**.
- **Wireless Setup**. This screen can be accessed through both the Setup menu on the Advanced screen and the dashboard on the Basic Home screen. For more information, see *Basic Wireless Setup* on page 30.
- **Guest Network**. This screen can be accessed through both the Setup menu on the Advanced screen and the dashboard on the Basic Home screen. For more information, see *Set Up a Guest Network* on page 39.
- **USB Storage**. For more information, see *Chapter 5, USB Storage*.
- **Security**. For more information, see *Chapter 6, Security*.
- **Administration**. For more information, see *Chapter 7, Administration*.
- **Advanced Setup**. For more information, see *Chapter 8, Advanced Settings*.
- **Advanced VPN**. For more information, see *Chapter 9, Virtual Private Networking*.

NETGEAR genie Advanced Home Screen

The genie ADVANCED Home dashboard presents status information. The content is the same as what is on the Router Status screen available from the Administration menu. The genie Advanced Home screen is shown in the following figure:



This screen is also displayed through the Administration menu.

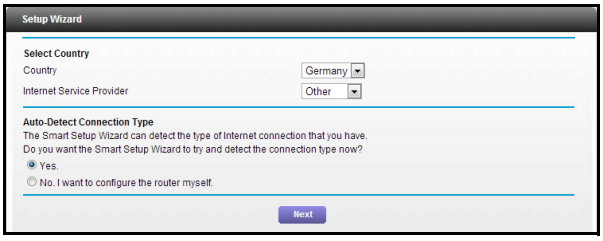
Setup Wizard

You can use the Setup Wizard to detect your Internet settings and automatically set up your modem router. The Setup Wizard is not the same as the genie screens that display the first time you connect to your modem router to set it up.

➢ **To use the Setup Wizard:**

1. Select **ADVANCED > Setup Wizard**.

   The Setup Wizard screen displays:

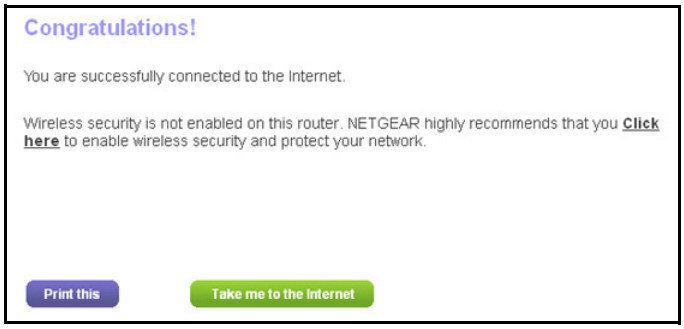


2. In the Country list, select your country.
3. In the Internet Service Provider list, select your internet service provider.
4. Select **Yes** and select your location.

   If you select No, you are taken to the Internet Setup screen (see *Internet Setup* on page 26).

5. Click **Next**.

   The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. The following screen displays:



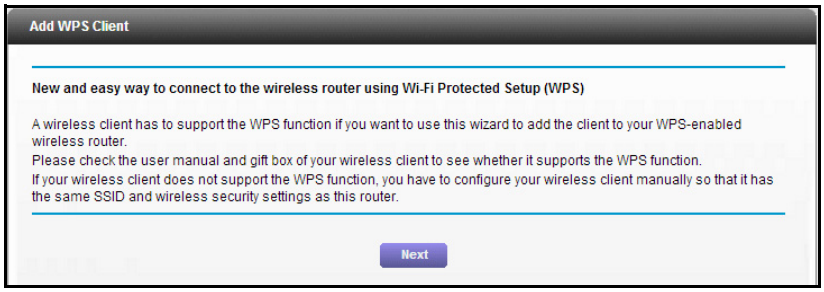
WPS Wizard

The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device, either press its **WPS** button or locate its WPS PIN.

➢ **To use the WPS Wizard:**

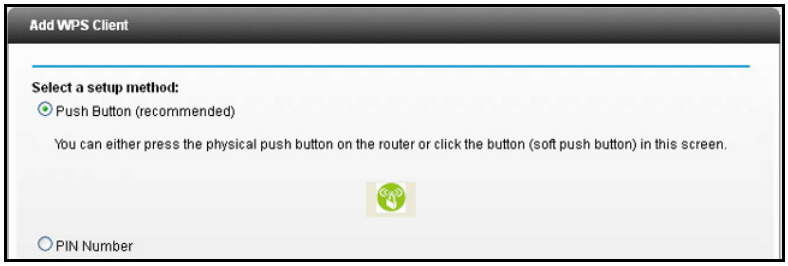
1. Select **ADVANCED > WPS Wizard**.

   The following screen displays:



2. Click **Next**.

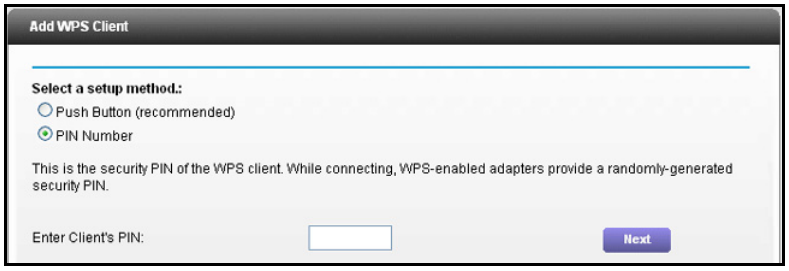
   The following screen lets you select the method for adding the WPS client (a wireless device or computer).



   You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.

- To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button on the front of the modem router. Within 2 minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
- To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.



Within 2 minutes, go to the client device and use its WPS software to join the network without entering a password.

The modem router attempts to add the WPS-capable device. The WPS LED on the front of the modem router blinks green. When the modem router establishes a WPS connection, the LED is solid green, and the modem router WPS screen displays a confirmation message.

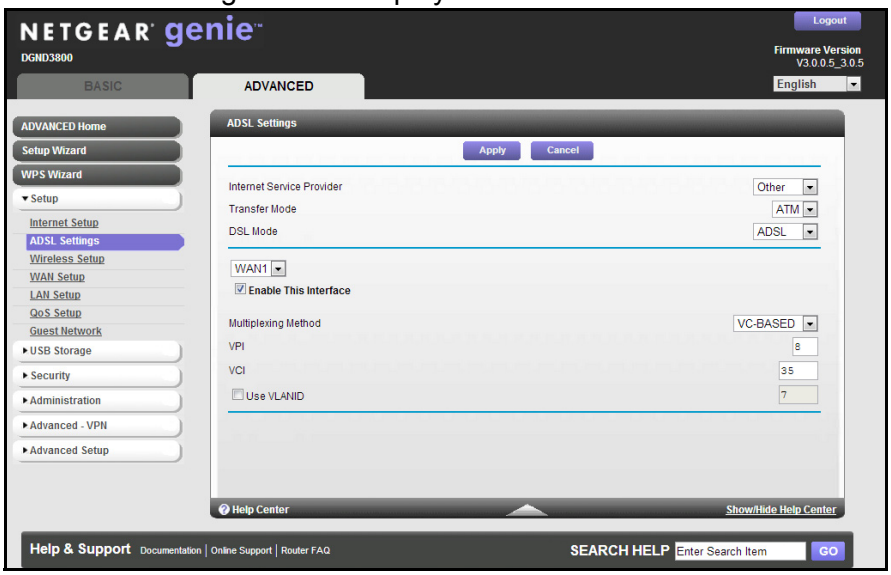
ADSL Setup

The ADSL Settings screen lets you configure the multiplexing method and the virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI) of your ADSL connection. The default parameters should be correct to match the system used by your ISP.

➢ **To enter a multiplexing method or VPI/VCI number (if provided by the ISP):**

1. Select **ADVANCED > Setup > ADSL Setup**.

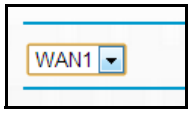
The ADSL Settings screen displays:



2. In the Internet Service Provider drop-down list, select your ISP.
3. Specify the transfer mode.

   The transfer mode can be PTM (Packet Transfer Mode) or ATM (Asynchronous Transfer Mode). The VDSL2 interface supports PTM. PTM transports packets (IP, PPP, Ethernet, MPLS, and so on) over DSL links as an alternative to using ATM. PTM is based on the Ethernet in the First Mile (EFM) IEEE802.3ah standard.

4. Select the DSL mode. The available settings depend on the selection in the Transfer Mode list.
   - If the Transfer Mode is ATM, the DSL mode can be Auto, ADSL, ADSL2, or ADSL2+.
   - If the transfer mode is PTM, the DSL mode is VDSL (Very-high-bit-rate digital subscriber line).
5. From the WAN connection drop down menu, select **WAN1**.



   - If the DSL port is plugged in, WAN1 is configured for DSL.
   - If the WAN Ethernet port is plugged in, WAN1 is configured for Ethernet.
   - If both the DSL port and WAN Ethernet port have been plugged in, only the DSL port is active and the WAN Ethernet port is disabled because only one WAN port can be active.

Note: WAN1 is for normal Internet access and WAN2 is for IPTV service. If you are subscribed to IPTV, you need to set up WAN2. The set up for WAN1 and WAN2 should be the same. If you are not subscribed to IPTV service, you do not need to set up WAN2. VLAN tags are used to distinguish the WAN1 and WAN2 traffic.

6. Select the **Enable This Interface** check box.

   If the **Enable This Interface** check box is not selected, this interface is not enabled.

7. In the Multiplexing Method drop-down list, select **LLC-based** or **VC-based**.
8. For the VPI, type a number between 0 and 255. The default is 8 for the U.S. version, 0 for the worldwide version, and 1 for the German version.
9. For the VCI, type a number between 32 and 65535. The default is 35 for the U.S. version, 38 for the worldwide version, and 32 for the German version.
10. (Optional) Select the **Use VLANID** check box.

    For WAN1, the default VLAN ID is 7.

    For WAN2, the default VLAN ID is 8.

    If you select the **Use VLANID** check box, a VLAND is added to all packets sent from LAN to WAN (DSLAM), and a VLAN ID is removed from all packets sent from WAN (DSLAM) to LAN.

Note: VALNID is for VDSL users (PTM mode). If you are using ADSL, and you are subscribed to IPTV service, select the **Use VLANID** check box and set up WAN1 and WAN2. If you are using ADSL, but you are not subscribed to IPTV service, do not select the **Use VLANID** check box and you do not have to set up WAN1 and WAN2. VLANID is used to distinguish IPTV traffic from the normal internet traffic.

11. Click **Apply**.

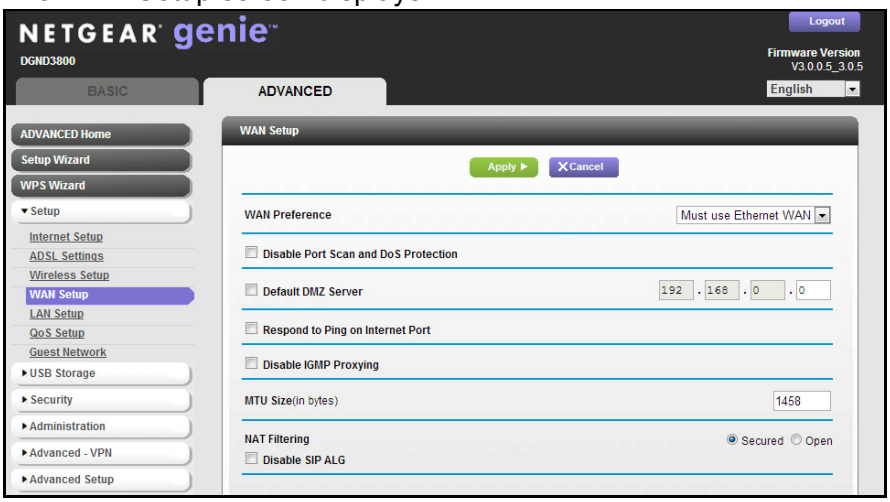
WAN Setup

You can use the WAN Setup screen to specify the ADSL or Ethernet port setting for your Internet connection, though by default the modem router automatically detects the Internet port. The WAN Setup screen also lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the modem router to respond to a ping on the WAN (Internet) port.

➢ **To view or change the WAN settings:**

1. Select **ADVANCED > Setup > WAN Setup.**

   The WAN Setup screen displays:



2. Specify the settings for your Internet connection.

   The fields in this screen are described in the following section.

3. Click **Apply**.

WAN Setup Screen Fields

The following fields are available:

- **WAN Preference**. By default this field is set to Auto-Detect so that the modem router automatically detects if the Internet connection is through the ADSL port or the Ethernet WAN port. You can use this field to select Must use DSL WAN or Must use Ethernet WAN.
- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.
- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*.
- **Respond to Ping on Internet Port**. If you want the modem router to respond to a ping from the Internet, select this check box. Use this feature only as a diagnostic tool because it allows your modem router to be discovered. Do not select this check box unless you have a specific reason.
- **Disable IGMP Proxying**. The IGPM proxying feature lets a LAN computer receive the multicast traffic directed to it from the Internet. Selecting this check box prevents this from occurring.

- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This is rarely required. You should change the setting in this field only if you are sure that it is necessary for your ISP connection. See *Change the MTU Size* on page 48.
- **NAT Filtering**. Network Address Translation (NAT) determines how the modem router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.
- **Disable SIP ALG**. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. Select the **Disable SIP ALG** check box to disable the SIP ALG. Disabling the SIP ALG might be useful when you are running certain applications.

Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The modem router recognizes some of these applications and works correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

WARNING:

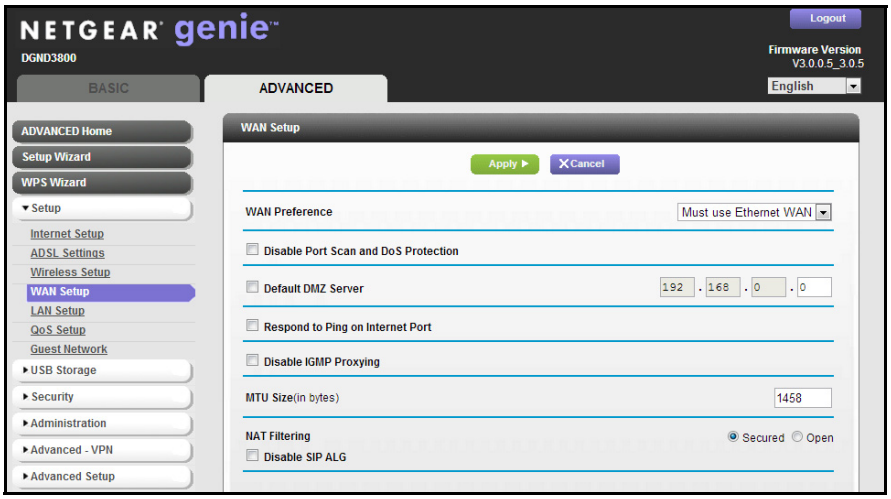
DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

The modem router discards traffic from the Internet that is not a response to one of your computers or a service that you have set up in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have the modem router forward the traffic to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. Select **ADVACNED > Setup > WAN Setup**.

The WAN Setup screen displays:



2. Select the **Default DMZ Server** check box.
3. Type the IP address.
4. Click **Apply**.

   Your changes are saved.

Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path has a lower MTU setting than the other devices, the data packets are split or “fragmented” to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal
  - America Online’s DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR modem routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➢ **To change the MTU size:**

1. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup screen displays.

2. In the MTU Size field, enter a value from 64 to 1500.
3. Click **Apply**.

   Your change is saved.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP). The modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is:

- **LAN IP address**. 192.168.0.1

- **Subnet mask**. 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications.

By default, the modem router acts as a DHCP server. The modem router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the modem router. The modem router tests each address before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the modem router are satisfactory.

The modem router delivers the following parameters to any LAN device that requests DHCP:

- IP address
- Subnet mask
- Gateway IP address (the modem router's LAN IP address)
- Primary DNS server (if specified in the Internet Setup screen); otherwise, the modem router's LAN IP address)
- Secondary DNS server if you entered this in the Internet Setup screen

If you change the LAN IP address of the modem router while connected through the browser, you are disconnected from the network.

➢ **To change the LAN settings:**

1. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup screen displays:

2. Specify the settings that you want to customize (see *LAN Setup Screen Settings*).
3. Click **Apply**.

   Your changes are saved.

LAN Setup Screen Settings

The following settings are available.

Device Name. By default, this is DGND3800B (the modem router model). You can change it to another name if you prefer.

LAN TCP/IP Setup

- **Device Name**. This is an abbreviated name of the modem router.
- **Use Auto IP**. Select this check box if you want the modem router to set up the LAN IP addresses automatically.
- **IP Address**. The LAN IP address of the modem router.
- **IP Subnet Mask**. The LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which addresses have to be reached through a gateway or modem router.

Use Router as DHCP Server

Usually, this check box is selected so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server. For more information, see *Specify DHCP Server Settings* on page 51.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it accesses the modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings. For more information, see *Address Reservation* on page 52.

Specify DHCP Server Settings

By default, the modem router is set up as a DHCP server. You can specify the range of addresses that the modem router assigns. You can also use another device on your network as the DHCP server, or specify the network settings of all of your computers.

➢ **To specify the pool of IP addresses that the modem router assigns:**

1. Select **ADVANCED > LAN Setup**.
2. Make sure that the **Use Router as DHCP Server** check box is selected.
3. Specify the range of IP addresses.

For example, using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

- In the Starting IP Address field, specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
- In the Ending IP Address field, specify the end of the range for the pool of IP addresses in the same subnet as the modem router.

4. Click **Apply**.

   Your changes are saved.

➢ **To disable the DHCP Server feature in the modem router:**

1. Select **ADVANCED > LAN Setup**.
2. Clear the **Use Router as DHCP Server** check box.
3. Click **Apply**.
4. If no DHCP server is on your network, set your computers' IP addresses manually so that they can access the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the modem router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. Select **ADVANCED > Setup > LAN Setup**.
2. In the Address Reservation section of the screen, click the **Add** button.
3. In the IP Address field, type the IP address to assign to the computer or server.

   Choose an IP address from the modem router's LAN subnet, such as 192.168.0.x.

4. Type the MAC address of the computer or server.

   Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

5. Click **Apply.**

   The reserved address is entered into the table.

   The reserved address is not assigned until the next time the computer contacts the modem router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

➢ **To edit or delete a reserved address entry:**

1. Select the radio button next to the reserved address you want to edit or delete.

2. Click **Edit** or **Delete**.

Quality of Service (QoS) Setup

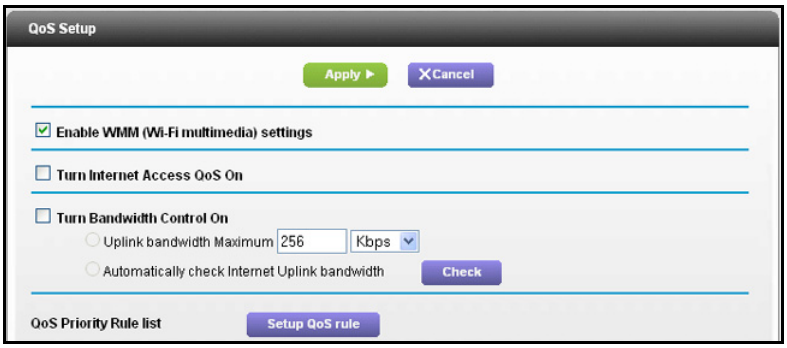
QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection.

WMM QoS for Wireless Multimedia Applications

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video. WMM QoS is enabled by default.

➢ **To disable WMM QoS:**

1. Select **ADVANCED > Setup > QoS Setup**.



2. Clear the **Enable WMM** check box.
3. Click **Apply**.

Set Up QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the modem router
- A specific device by MAC address

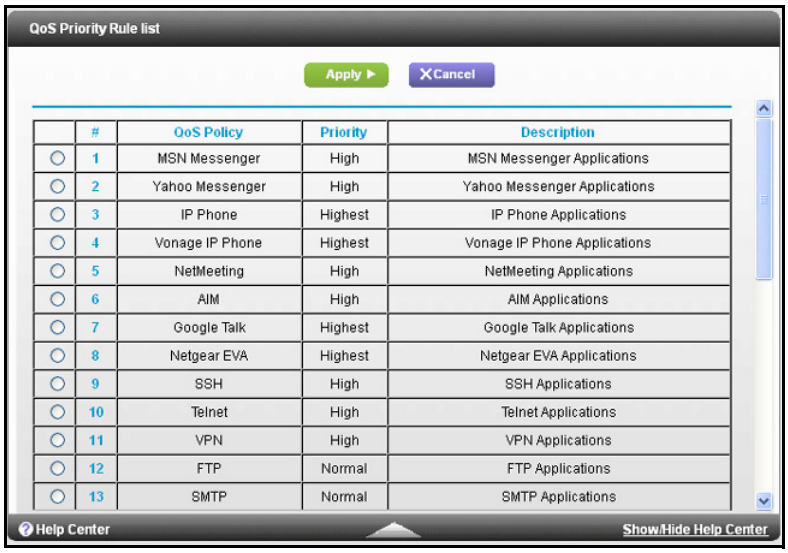
To specify prioritization of traffic, create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

➢ **To create a QoS policy for applications and online games:**

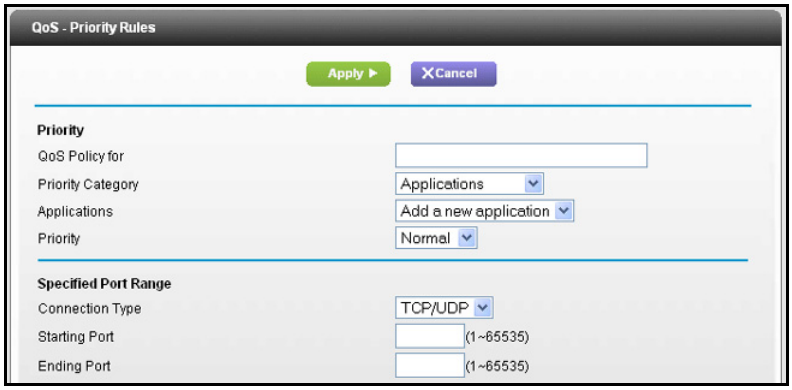
1. Select **ADVANCED > Setup > QoS Setup.**
2. Select the **Turn Internet Access QoS On** check box.
3. Click the **Setup QoS Rule** button.

   The QoS Priority Rule list displays.



   You can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. You can also delete all the rules by clicking the **Delete All** button.

4. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule**.



5. In the QoS Policy for field, type the name of the application or game.
6. In the Priority Category list, select either **Applications** or **Online Gaming**.

A list of applications or games displays.

7. Select an existing item from the list, scroll and select **Add a New Application**, or **Add a New Game**, as applicable.
8. If prompted, in the Connection Type list, select either **TCP**, **UDP**, or both (**TCP/UDP**).

   Specify the port number or range of port numbers that the application or game uses.
9. From the Priority list, select the priority for Internet access for this traffic relative to other applications and traffic.

   The options are Low, Normal, High, and Highest.
10. Click **Apply.**

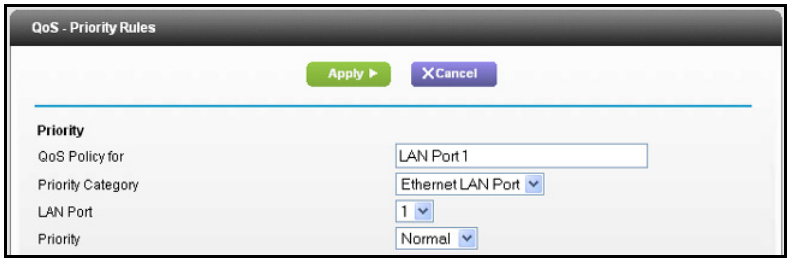
    The rule is saved in the QoS Policy list.

    The QoS Setup screen displays.

QoS for a Modem Router LAN Port

➢ **To create a QoS policy for a device connected to a LAN port:**

1. Select **ADVANCED > Setup > QoS Setup**.
2. Select the **Turn Internet Access QoS On** check box.
3. Click the **Setup QoS Rule** button.
4. Click the **Add Priority Rule** button.
5. From the Priority Category list, select **Ethernet LAN Port**.



6. From the QoS Policy for list, select the LAN port.
7. From the Priority list, select the priority for Internet access for this port's traffic relative to other applications.

   The options are Low, Normal, High, and Highest.
8. Click **Apply**

   The rule is saved in the QoS Policy list.

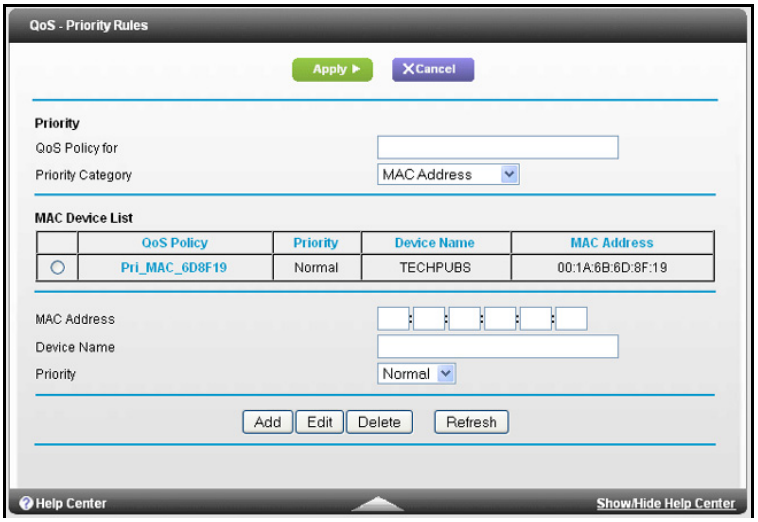
   The QoS Setup screen displays.
9. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

1. Select **ADVANCED > Setup > QoS Setup**.
2. Click the **Setup QoS Rule** button.

   The QoS Setup screen displays.
3. Click **Add Priority Rule**.
4. From the Priority Category list, select **MAC Address**.



5. If the device to be prioritized appears in the MAC Device List, select its radio button.

   The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, fill in these fields manually.
6. From the Priority list, select the priority for Internet access for this device's traffic relative to other applications and traffic.

   The options are Low, Normal, High, and Highest.
7. Click **Apply**.

   This rule is saved in the QoS Policy list.

   The QoS Setup screen displays.
8. Select the **Turn Internet Access QoS On** check box.
9. Click **Apply**.

Edit or Delete an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **ADVANCED > QoS Setup**.

2. Select the radio button next to the QoS policy that you want to edit or delete, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply**.

   Your changes are saved in the QoS Setup screen.

USB Storage

5

This chapter describes how to access and configure a USB storage drive attached to your modem router. The USB port on the modem router can be used to connect only USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, CD drives, or DVD drives to the modem router USB port.

This chapter contains the following sections:

- *USB Drive Requirements*
- *Connect a USB Storage Device to the Modem Router*
- *Access the USB Storage Device*
- *File-Sharing Scenarios*
- *View a USB Device Attached to the Modem Router*
- *USB Storage Device Network and Access Settings*
- *Available Network Folders*
- *Media Server Settings*
- *Specify Approved USB Devices*
- *Connect to the USB Drive from a Remote Computer*
- *Connect to the USB Drive with Microsoft Network Settings*
- *Enable File and Printer Sharing*
- *Safely Remove a USB Drive*

For more information about ReadySHARE features, visit *www.netgear.com/readyshare*.

USB Drive Requirements

The modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table. Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables.

Table 3. USB drive speeds

Bus	Speed/Sec
USB 1.1	12 Mbits
USB 2.0	480 Mbits

The modem router works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB drives that the modem router supports, visit: *http://kbserver.netgear.com/readyshare.*

The modem router supports both read and write for FAT16, FAT32, NTFS, and Linux file systems (EXT2).

Note: Some USB external hard drives and flash drives require you to load the drivers onto the computer before the computer can access the USB device. Such USB devices do not work with the modem router.

Connect a USB Storage Device to the Modem Router

ReadySHARE lets you access and share or a USB drive connected the modem router USB port. If your USB device has special drivers, it is not compatible.

➢ **To connect a USB storage device:**

1. Insert your USB storage device into the USB port on the rear or front panel of the modem router.

2. If your USB device has a power supply, you must use it when you connect the USB device to the modem router.

It might take up to 2 minutes before the USB device is ready for sharing.

Access the USB Storage Device

When you connect the USB device to the modem router USB port, it might take up to 2 minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).

- **To access the USB device from a Mac:**

  1. Select **Go > Connect to Server**.
  2. Enter **smb://readyshare** as the server address.
  3. Click **Connect**.

- **To access the USB device from Windows:**

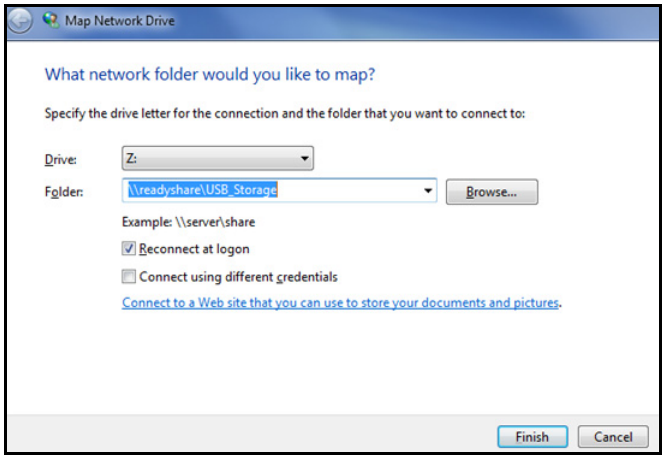
  Use any of these methods to access the USB device:

  - Select **Start > Run**. Enter **\\readyshare** in the dialog box and click **OK**.
  - Open a browser and enter **\\readyshare** in the address bar.
  - Open My Network Places and enter **\\readyshare** in the address bar.

- **To map the USB device to a Windows network drive:**

  1. Visit *www.netgear.com/readyshare.*
  2. In the ReadySHARE USB Storage Access pane, click **PC Utility**.

     The readyshareconnect.exe file is downloaded to your computer.
  3. Launch readyshareconnect.exe.



  4. Select the drive letter to map to the network folder.
  5. (Optional) If you want to connect to the USB drive as a different user, select the **Connect using different credentials** check box.

     a. Type the user name and password that you want to use.

b. Click **OK**.

6. Click **Finish**.

   The USB drive is mapped to the drive letter that you specified.

➢ **To access the USB drive from a remote computer:**

1. Launch a web browser.
2. Connect using the modem router's Internet port IP address.

   If you are using Dynamic DNS, you can type the DNS name, rather than the IP address. You can view the modem router's Internet IP address on the Basic Home screen (see *Dashboard (BASIC Home Screen)* on page 22).

➢ **To access the USB drive with FTP from a remote computer:**

1. Make sure that the FTP check box is selected in the Access Method section of the USB Storage (Advanced Settings) screen (see *USB Storage Device Network and Access Settings* on page 63).
2. Launch a web browser.
3. Type **ftp://** and the Internet port IP address in the address field of the browser.

   For example, type **ftp://10.1.65.4**.

   If you are using Dynamic DNS, you can type the DNS name rather than the IP address.
4. Type the account name and password for the account that has access rights to the USB drive.

   The user name (account name) for All – no password is **guest**.

   The folders on the USB drive that your account has access to display. For example, you could see: share/partition1/directory1. You can read and copy files from the USB folder.

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any Windows, Mac, or Linux file type including text, Word, PowerPoint, Excel, MP3, pictures, and multimedia files. USB drive applications include:

- Sharing multimedia with friends and family such as MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network. You can store files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and Windows computers by using the USB drive as a go-between across the systems.
- Sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Share Photos

You can create your own central storage location for photos and multimedia. This method eliminates the need to log in to (and pay for) an external photo-sharing site.

➢ **To share files with your friends and family:**

1. Insert your USB drive into the USB port on the modem router either directly or with a USB cable.

   Computers on your local area network (LAN) can automatically access this USB drive using a web browser or Microsoft Networking.

2. If you want to specify read-only access or to allow access from the Internet, see *USB Storage Device Network and Access Settings* on page 63.

Store Files in a Central Location for Printing

This scenario is for a family that has one high-quality color printer directly attached to a computer, but not shared on the local area network (LAN). This family does not have a print server.

- One family member has photos on a Macintosh computer that she wants to print.
- The photo-capable color printer is directly attached to a computer, but not shared on the network.
- The Mac and computer are not visible to each other on the network.

➢ **To print photos from a Mac on the printer attached to a computer:**

1. On the Mac, access the USB drive by typing **\\readyshare** in the address field of a web browser. Then copy the photos to the USB drive.
2. On the computer, use a web browser or Microsoft Networking to copy the files from the USB drive to the computer. Then print the files.

Share Large Files over the Internet

Sending files that are larger than 5 MB can pose a problem for many email systems. The modem router allows you to share large files such as PowerPoint presentations or .zip files over the Internet. FTP can be used to download shared files from the modem router.

Sharing files with a remote colleague involves the following considerations:

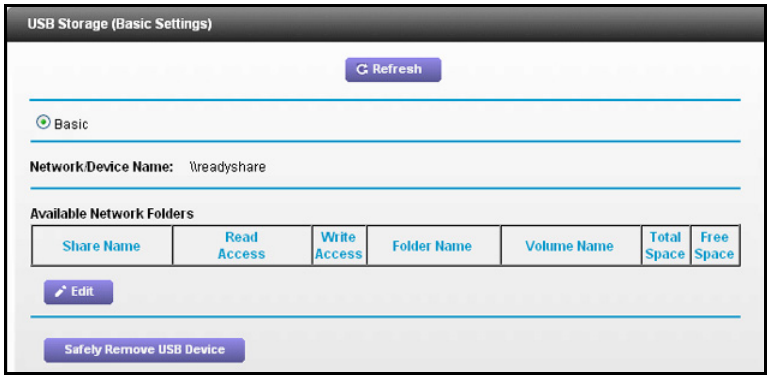
- There are two user accounts: admin and guest. The password for admin is the same one that you use to access the modem router. By default, it is **password**. The guest user account has no password.
- On the FTP site, the person receiving the files uses the guest user account and enters the password. (FTP requires that you type something in the password field.)
- Be sure to select the **FTP (via Internet)** check box in the USB Storage (Advanced Settings) screen. This option supports both downloading and uploading of files.

You can enable the HTTP (via Internet) option on the USB Storage (Advanced Settings) screen to share large files. This option supports downloading files only.

View a USB Device Attached to the Modem Router

➢ **To view basic information about the USB storage device:**

1. Select **BASIC > ReadySHARE**.



   By default, the Basic radio button is selected, and the screen displays a USB storage device if it is attached to the modem router USB port.

   If you logged in to the modem router before you connected your USB device, you might not see your USB device in this screen. If this happens, log out and then log back in.

2. (Optional) To view the files and folders on the USB device, click the network device name or the share name.
3. (Optional) To view more detail or to change the USB device settings, click **Edit**.

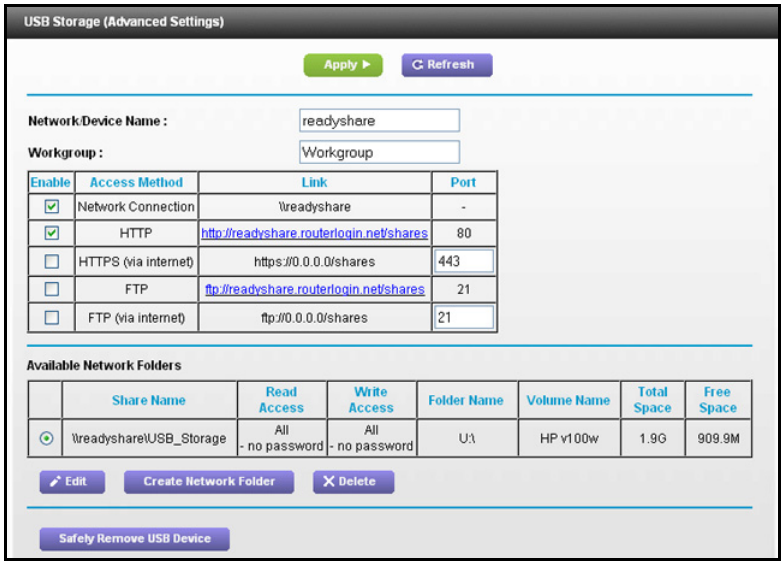
   The USB Storage (Advanced Settings) screen displays. See *USB Storage Device Network and Access Settings* on page 63.

USB Storage Device Network and Access Settings

You can set up the device name, workgroups, and network folders for your USB device.

➢ **To view or change the USB storage advanced settings:**

1. Select **ADVANCED > USB Storage > Advanced Settings**.



2. Specify access to the USB storage device.
   - **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the modem router.
   - **Workgroup**. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.
   - **Access Method**. Select the check boxes for the access methods that you want.
     - **Network Neighborhood/MacShare**. Enabled by default.
     - **HTTP**. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.
     - **HTTPS (via Internet)**. Disabled by default. If you enable this setting, remote users can type http://<public IP address/shares> (for example, http://1.1.10.102/shares) or a URL domain name to access the USB drive over the Internet. This feature supports file uploading only.
     - **FTP**. Disabled by default.
     - **FTP (via Internet)**. Disabled by default. If you select this feature, remote users can access the USB drive through FTP over the Internet. This setting supports both downloading and uploading of files.
3. If you changed the settings, click **Apply**.

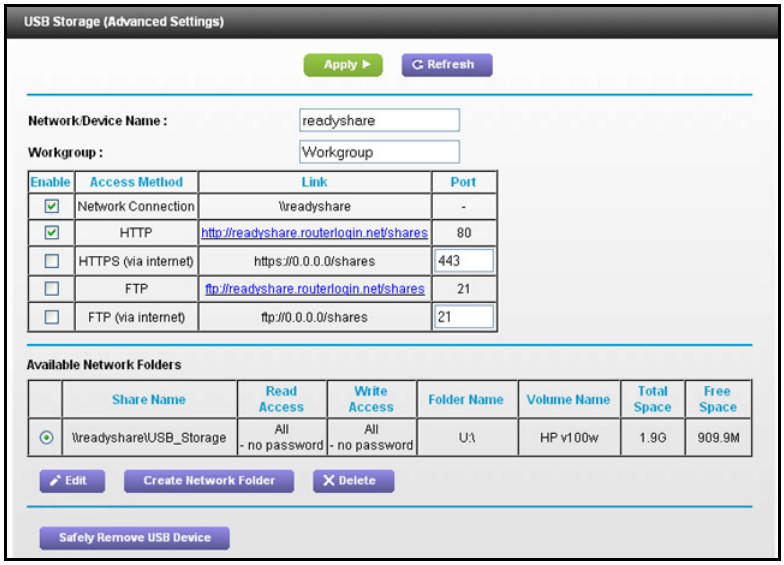
   Your changes are saved.

Available Network Folders

You can view or change the network folders on the USB storage device.

➢ **To view network folders:**

1. Select **ADVANCED > USB Storage > Advanced Settings**.



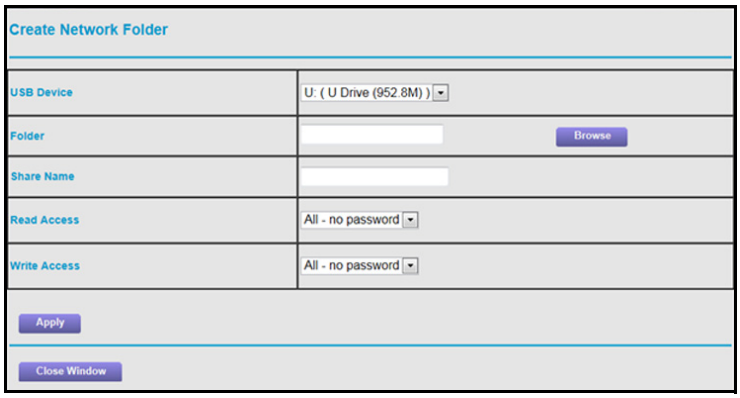
2. Scroll down to the Available Networks Folder section of the screen.
   - **Share Name**. If only one device is connected, the default share name is USB_Storage. (Some router models have more than one USB port.)

     You can click the name, or you can type it in the address field of your web browser. If Not Shared is shown, the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.
   - **Read Access and Write Access**. Show the permissions and access controls on the network folder: All – no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the modem router.
   - **Folder Name**. Full path of the network folder.
   - **Volume Name**. Volume name from the storage device (either USB drive or HDD).
   - **Total Space and Free Space**. Show the current utilization of the storage device.

➢ **To add a network folder:**

1. Select **ADVANCED > USB Storage > Advanced Settings**.

2. Click **Create Network Folder**.



   If the Add a Network Folder screen does not display, your web browser might be blocking pop-ups. If it is, then change the browser settings to allow pop-ups.

3. Click **Browse**.
4. Select the folder.
5. Fill in the Share Name field.
6. In the Read Access list and the Write Access list, select the setting that you want.

   The user name (account name) for All – no password is guest. The password for admin is the same one that is used to log in to the modem router. By default, it is password.

7. Click **Apply**.

   The folder is added on the USB device.

➢ **To edit a network folder:**

1. Select **ADVANCED > USB Storage > Advanced Settings**.
2. Click the **Edit** button.

   The Edit Network Folder screen displays the same settings shown in the Add a Network Folder screen.

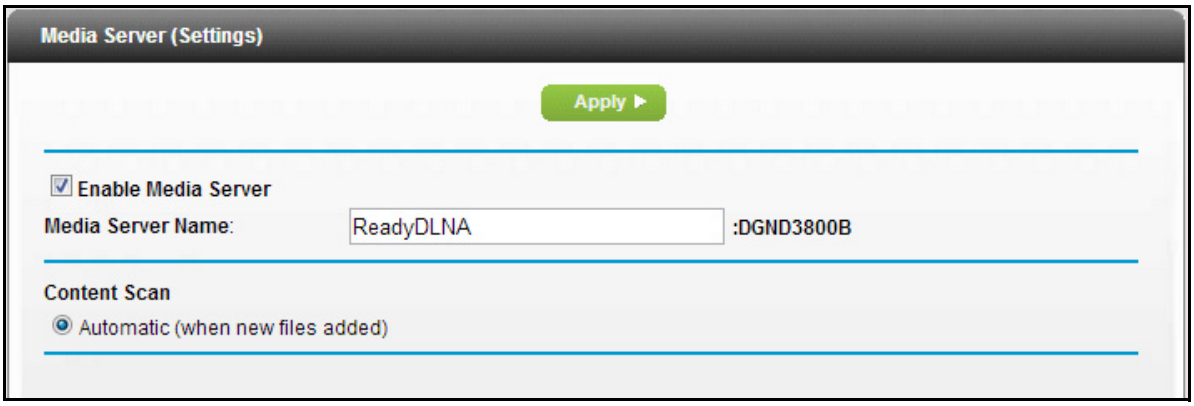
3. Change the settings in the fields as needed.
4. Click **Apply**.

   Your changes are saved.

Media Server Settings

By default, the modem router is set up to act as a Ready DLNA Media server, which lets you view movies and photos on DLNA/UPnP AV–compliant media players, such as Xbox360, Playstation, and NETGEAR's Digital Entertainer Live.

To view these settings, select **Advanced > USB Storage > Media Server** to display the following screen:



By default the Enable Media Server check box and the Automatic (when new files are added) radio button are selected. When these options are selected, the modem router scans for media files whenever new files are added to the ReadySHARE USB hard drive.

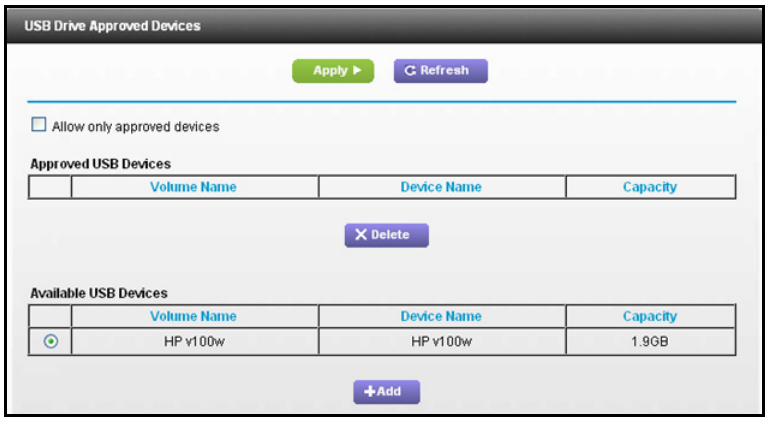
Specify Approved USB Devices

For more security, you can set up the modem router to share only approved USB devices.

➢ **To set up approved USB devices:**

1. Select **ADVANCED > Advanced Setup > USB Settings**.

2. Click the **Approved Devices** button.



This screen shows the approved USB devices and the available USB devices. You can remove or add approved USB devices.

3. In the Available USB Devices list, select the drive that you want to approve.
4. Click **Add**.
5. Select the **Allow only approved devices** check box.
6. Click **Apply**.

   Your change takes effect.

If you want to work with another USB device, first click the **Safely Remove USB Device** button for the currently connected USB device. Connect the other USB device, and repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a web browser, you use the modem router's Internet port IP address.

➢ **To connect to the modem router's USB drive using a web browser:**

1. First, locate the Internet port IP address. You can view this in the Router Status screen.
   a. Select **ADVANCED > Administration > Router Status**.
   b. Record the IP address that is listed for the Internet port. This is the IP address you can use to connect to the modem router remotely.
2. Use a web browser to connect to the modem router by typing **ftp://** and the Internet port IP address in the address field.

   For example, type **ftp://10.1.65.4**. If you are using Dynamic DNS, you can type the DNS name rather than the IP address.
3. Type the name and password of the account that has access rights to the USB drive.

   The directories of the USB drive that your account has access to display, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connect to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft Networking settings. You have to be running Microsoft Windows 7, Windows XP, Windows 2000,or older versions of Windows with Microsoft Networking enabled. You can use normal Explorer operations such as dragging and dropping, opening files, or cutting and pasting files from:

- Microsoft Windows Start menu, Run option
- Windows Explorer
- Network Neighborhood or My Network Place

Enable File and Printer Sharing

Each computer's network properties have to be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft Networking have to be enabled, as described in the following sections.

Note: In Windows 7, Windows XP, and Windows 2000, File and Printer Sharing is enabled by default.

Configure Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right-click **Network Neighborhood** and then select **Properties**. File and Printer Sharing for Microsoft Windows should be listed. If it is not, click **Add** and follow the installation prompts.

Note: If you have any questions about File and Printer Sharing, contact Microsoft for assistance.

Configure Windows 7, Windows XP, Windows 2000

Right-click the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If it is not, click **Install** and follow the installation prompts.

Safely Remove a USB Drive

If you want to physically disconnect a USB drive from the modem router USB port, first, log in to the modem router and safely remove it.

- **To remove a USB disk drive safely:**

  1. Select **ADVANCED > USB Storage > Basic Settings**.
  2. Click the **Safely Remove USB Device** button.

     This takes the drive offline.
  3. Physically disconnect the USB drive.

Security

6

This chapter explains how to use the basic firewall features of the modem router to prevent objectionable content from reaching the computers and devices on your network.

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Block Services (Port Filtering)*
- *Set Up Firewall Rules to Control Network Access*
- *Schedule When to Block the Internet*
- *Security Event Email Notifications*

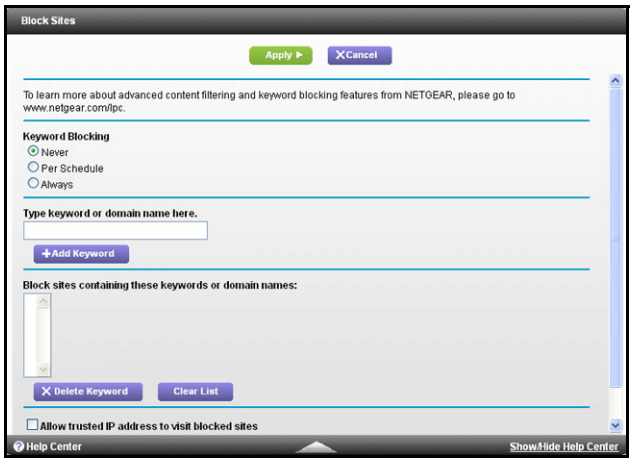
> **Note:** The Parental Controls screen can be accessed through both the Security menu on the Advanced screen and the dashboard on the Basic Home screen. For more information about Parental Controls, see *Parental Controls* on page 36.

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

➢ **To set up keyword blocking:**

1. Select **ADVANCED > Security > Block Sites**.



2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain and click **Add Keyword**.

   The Keyword list supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.
4. Click **Apply**.

➢ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword.**
3. Click **Apply**.

   Your changes are saved.

➢ **To specify a trusted computer:**

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply**.

Your changes are saved.

Block Services (Port Filtering)

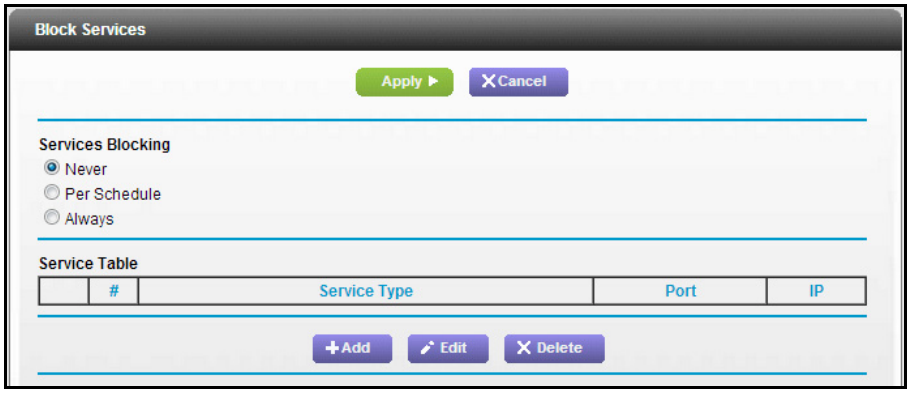
Services are functions that server computers perform at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with the destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 - 65535 by the authors of the application. Although the modem router already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Block Services screen lets you add and block specific Internet services by computers on your network. This is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers the application uses.

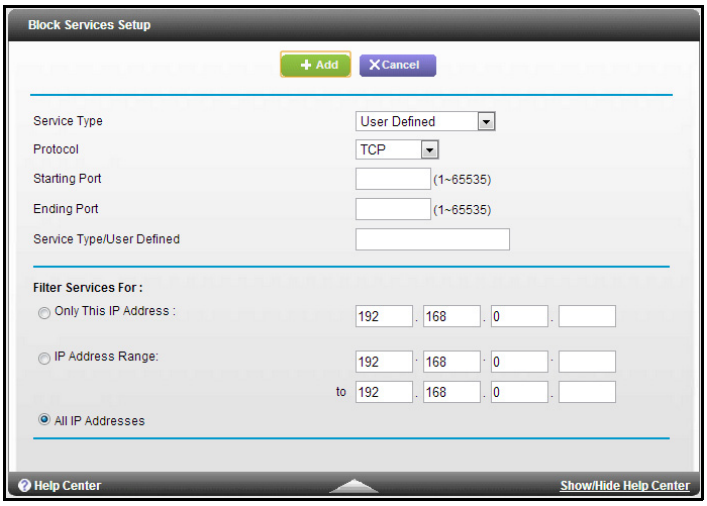
➢ **To block services:**

1. Select **ADVANCED > Security > Block Services**.



2. Select either **Per Schedule** or **Always**.
3. If you selected Per Schedule, specify a time period in the Schedule screen.
4. Click the **Add** button.

The Block Services Setup screen displays:



5. From the Service Type list, select the application or service to allow or block.

   The list displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.

6. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **TCP/UDP (Both)**.
7. Enter the starting and ending port numbers.

   If the application uses a single port number, enter that number in both fields.

8. Select the radio button for the IP address configuration you want to block, and enter the IP addresses.

   You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network.

9. Click the **Add** button.

   Your changes are saved.

Set Up Firewall Rules to Control Network Access

By default your router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. You might need to create exceptions to this rule to allow remote computers to access a server on your local network or to allow certain applications and games to work correctly. Your router provides port forwarding and port triggering for creating these exceptions.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and

process information. Before forwarding your message to the remote computer, your router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser and your operating system assigns port number 5678 to this browser session.
2. You type http://www.example.com into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.

   Source address. Your computer's IP address.

   Source port number. 5678, which is the browser session.

   Destination address. The IP address of www.example.com, which your computer finds by asking a DNS server.

   Destination port number. 80, which is the standard port number for a web server process.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
   - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
   - The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

   Your router then sends this request message through the Internet to the web server at www.example.com.
4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. The public IP address of your router.

   Destination port number. 33333.
5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

Source address. The IP address of www.example.com.

Source port number. 80, which is the standard port number for a web server process.

Destination address. Your computer's IP address.

Destination port number. 5678, which is the browser session that made the initial request.

Port Triggering to Open Incoming Ports

Some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your modem router, you can tell the modem router to open more incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the modem router, "When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your modem router.
3. Your modem router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your modem router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your modem router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your modem router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an "identify" message to your modem router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the modem router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your modem router checks its session table and learns that there is an active session for port 113, associated with your computer. The modem router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.
8. When you finish your chat session, your modem router eventually senses a period of inactivity in the communications. The modem router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or the relevant user groups or news groups.

Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your modem router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the modem router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.0.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your modem router. The remote computer composes a web page request message with the following destination information:

   Destination address. The IP address of www.example.com, which is the address of your modem router.

   Destination port number. 80, which is the standard port number for a web server process.

   The remote computer then sends this request message through the Internet to your modem router.

2. Your modem router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.0.123. Therefore, your modem router modifies the destination information in the request message:

   The destination address is replaced with 192.168.0.123.

   Your modem router then sends this request message to your local network.

3. Your web server at 192.168.0.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your modem router.
4. Your modem router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups or news groups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- With port triggering, the modem router does not need to know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

The port forwarding feature lets you allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

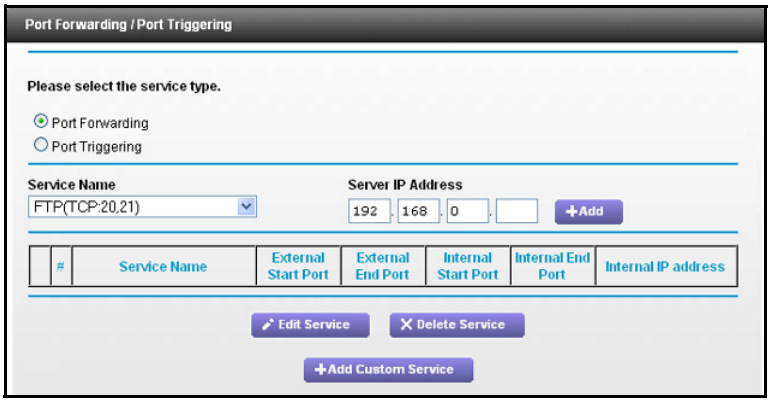
Use the Port Forwarding/Port Triggering screen to configure the modem router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before you start, determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

To ensure that your server computer always has the same IP address, use the reserved IP address feature of your product. See *Address Reservation* on page 52.

➢ **To forward specific incoming protocols:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.



2. Select the Port Forwarding radio button as the service type.
3. From the Service Name list, select the service or game that you will host on your network.

   If the service does not appear in the list, see *Add a Custom Service* on page 78.
4. In the Server IP Address field, enter IP address of your local computer that will receive the inbound traffic covered by this rule.
5. Click **Add**.

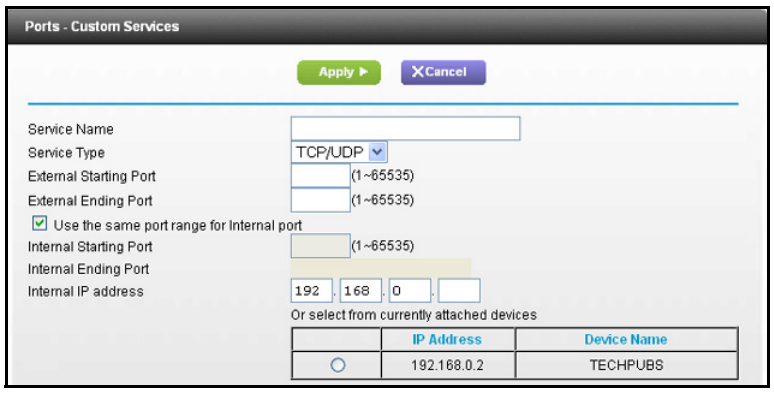
   The service appears in the list on the Port Forwarding screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, first determine which port number or range of numbers the application uses. You can usually determine this information by contacting the publisher of the application or user groups or news groups. When you have the port number information, follow these steps.

➢ **To add a custom service:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select the **Port Forwarding** radio button as the service type.
3. Click the **Add Custom Service** button.



4. In the Name field, enter a descriptive name.
5. In the Service Type list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the External Starting Port field, enter the beginning port number.
   - If the service uses only one port, enter the port number in the Ending Port field.
   - If the service uses a range of ports, enter the end port number in the Ending Port field.
7. In the Internal Starting Port field, enter the beginning port number.
   - If the service uses only one port, enter the port number in the Ending Port field.
   - If the service uses a range of ports, enter the end port number in the Ending Port field
8. In the Internal IP Address field, enter the IP address of your local computer that will provide this service.
9. Click **Apply**.

   The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Make a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

   In this example, your modem router always gives your web server an IP address of 192.168.0.33.

2. In the Port Forwarding/Port Triggering screen, configure the modem router to forward the HTTP service to the local address of your web server at **192.168.0.33**.

   HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your modem router to use the name.

   To access your web server from the Internet, a remote user has to know the IP address that your ISP assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the modem router monitors outbound traffic looking for a specified outbound “trigger” port. When the modem router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The modem router then temporarily opens the specified incoming port or ports and forwards incoming traffic on the triggered ports to the triggering computer.

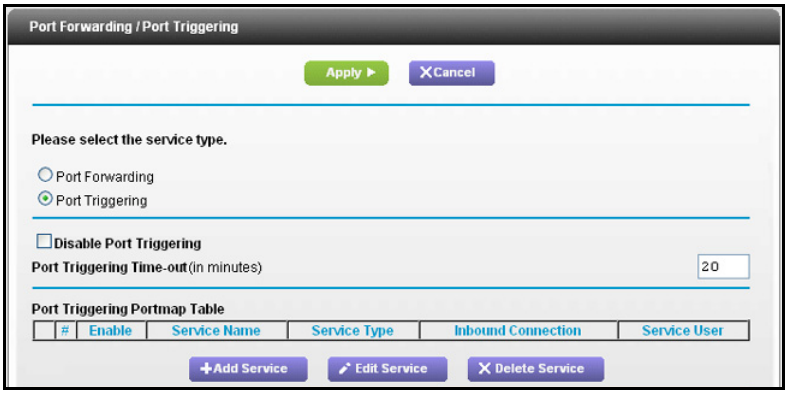
Port forwarding creates a static mapping of a port number or range to a single local computer. Port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP).

To configure port triggering, you need to know which inbound ports the application needs, and the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or news groups.

➢ **To enable port triggering:**

1. Select **ADVANCED > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button.



3. Clear the **Disable Port Triggering** check box.

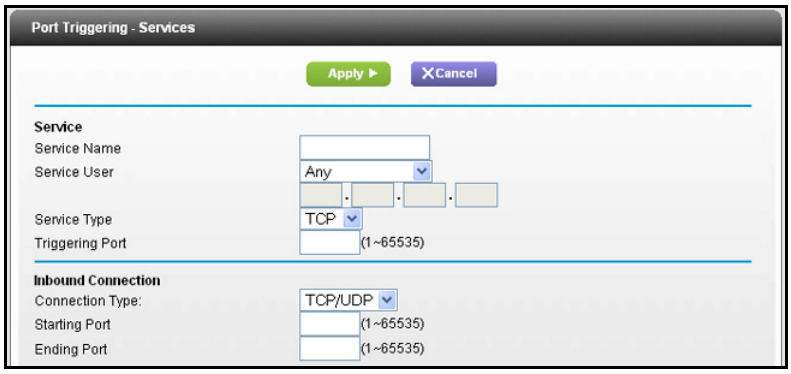
Note: If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the modem router is retained even though it is not used.

4. In the Port Triggering Timeout field, enter a value up to 9999 minutes.

   This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the modem router cannot detect when the application has terminated.

➢ **To add a port triggering service:**

1. On the Port Triggering screen, click **Add Service**.



2. In the Service Name field, type a descriptive service name.
3. In the Service User list, select **Any**, or select **Single address** and enter the IP address of one computer.
   - **Any** (the default), allows any computer on the Internet to use this service.
   - **Single address** restricts the service to a particular computer.
4. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**).

   If you are not sure, select TCP/UDP.
5. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.
6. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
7. Click **Apply**.

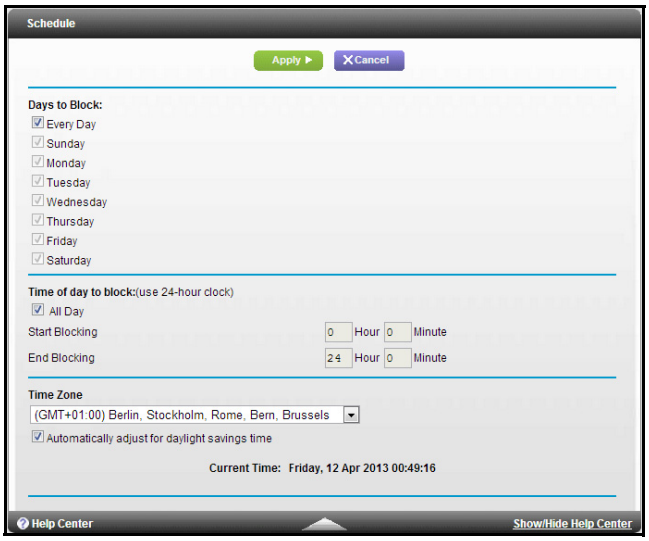
   The service appears in the Port Triggering Portmap Table.
8. Make sure that you enable port triggering so that the service that you added will be used.

Schedule When to Block the Internet

You can specify the days and time that you want to block Internet access.

➢ **To schedule blocking:**

1. Select **ADVANCED > Security > Schedule**.



2. Set up the schedule for blocking keywords and services.
   - **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
   - **Time of Day to Block**. Select a start and end time in 24-hour format, or select **All Day** for 24-hour blocking.
3. Select your time zone from the list.

   If you use daylight savings time, select the **Automatically adjust for daylight savings time** check box.
4. Click **Apply**.

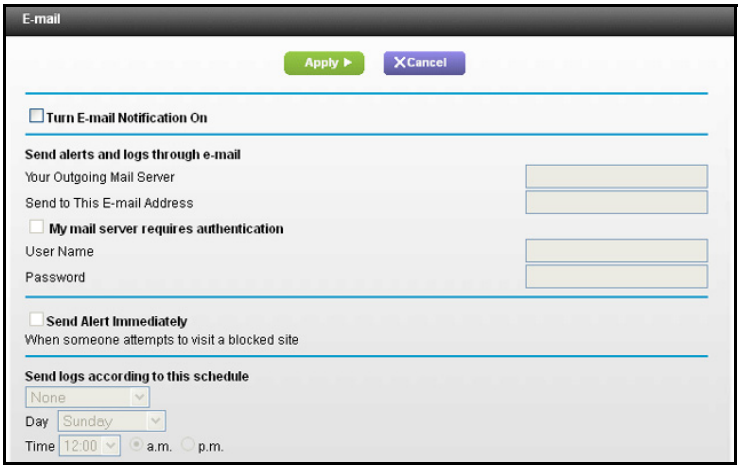
   Your settings are saved.

Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the E-mail screen, and specify which alerts you want to receive and how often.

➢ **To set up email notifications:**

1. Select **ADVANCED > Security > E-mail**.



2. Select the **Turn Email Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com).

   You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent.
4. Enter the email address to which logs and alerts are sent in the Send to This Email Address field.

   This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box.

   Fill in the User Name and Password fields for the outgoing email server.
6. (Optional) Select the **Send Alerts Immediately** check box.

   Email alerts are sent immediately when someone attempts to visit a blocked site.
7. (Optional) Fill in the fields in the Send logs according to this schedule section of the screen.

   Logs are sent automatically. If the log fills up before the specified time, the log is emailed. After the log is sent, the log is cleared from the modem router memory. If the modem router cannot email the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.
8. Click **Apply**.

   Your settings are saved.

Administration

7

This chapter describes the modem router settings for administering and maintaining your modem router and home network. For information about upgrading or checking the status of your modem router over the Internet, see *Remote Management* on page 109. For information about monitoring Internet traffic, See *Traffic Meter* on page 119.

This chapter includes the following sections:

- *Update the Modem Router Firmware*
- *View Router Status*
- *View Logs of Web Access or Attempted Web Access*
- *Manage the Configuration File*
- *Change the Password*

Note: The Attached Devices screen can be accessed through both the Administration menu on the Advanced screen and the dashboard on the Basic Home screen. For more information about attached devices, see *View Attached Devices* on page 35.

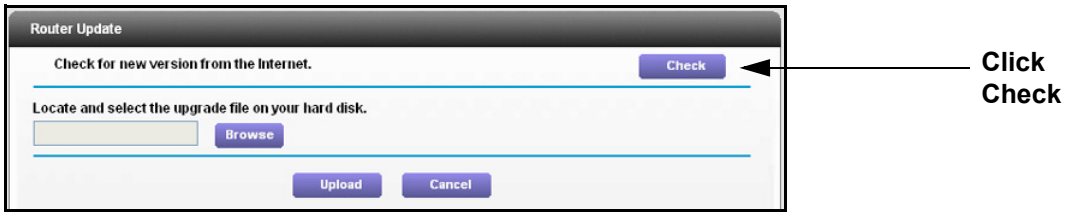
Update the Modem Router Firmware

The modem router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the Advanced tab. You might see a message at the top of the genie screens when new firmware is available for your product.

You can use the Check button on the Router Update screen to check and update to the latest firmware for your product if new firmware is available.

➢ **To check for new firmware and update your modem router:**

1. Select **ADVANCED > Administration > Router Update**.



2. Click **Check**.

   The modem router finds new firmware information if any is available.

3. Click **Yes**.

   The modem router locates the firmware you downloaded (the file ends in .img) and begins the update.

WARNING:

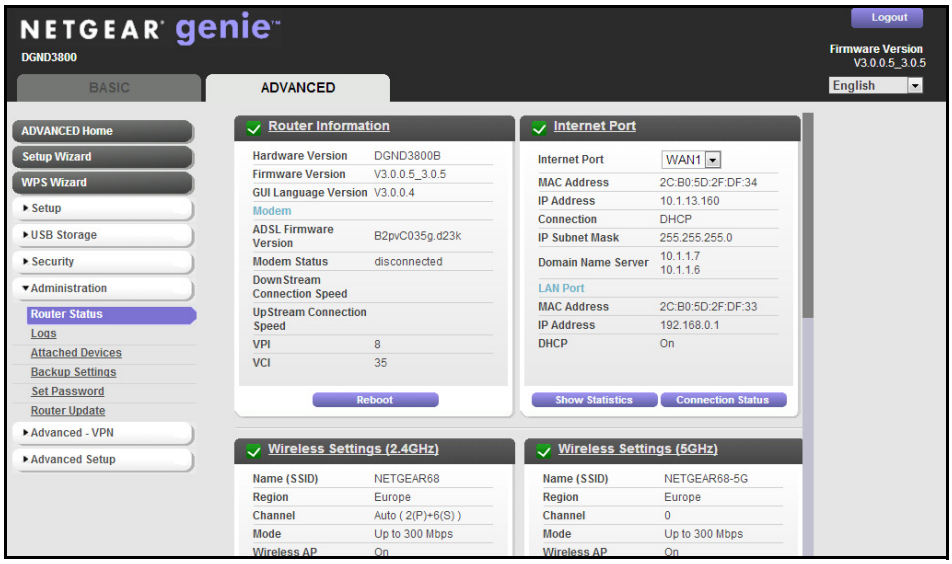
When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

When the upload is complete, your modem router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

View Router Status

➤ **To view modem router status and usage information:**

Select **ADVANCED Home** or select **Administration > Router Status**.



Router Information

Hardware Version. The modem router model.

Firmware Version. The version of the modem router firmware. It changes if you upgrade the modem router firmware.

GUI Language Version. The localized language of the user interface.

Modem. The current modem status and settings are shown in this section.

- **ADSL Firmware Version**. This is the version number of the low-level ADSL firmware. This is contained within the router firmware.
- **Modem Status**. The current state of the ADSL connection speed to your phone company.
- **DownStream Connection Speed**. The connection speed of the ADSL connection from your phone company to your router.
- **UpStream Connection Speed**. The connection speed of the ADSL connection form your router to the phone company.
- **VPI**. The VPI setting entered on the AFDSL Settings screen.
- **VCI**. The VCI setting entered on the ADSL Settings screen.

Internet Port

Internet Port. These are the current settings that you set in the Setup Wizard or Basic Settings screen.

MAC Address. The Media Access Control address, which is the unique physical address used by the Internet (WAN) port of the modem router.

IP Address. The IP address used by the Internet (WAN) port of the modem router. If no address is shown or the address is 0.0.0, the modem router cannot connect to the Internet.

Connection. This shows if the modem router is using a fixed IP address on the WAN. If the value is DHCP Client, the modem router obtains an IP address dynamically from the ISP.

IP Subnet Mask. The IP subnet mask used by the Internet (WAN) port of the modem router.

Domain Name Server. The Domain Name Server addresses used by the modem router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

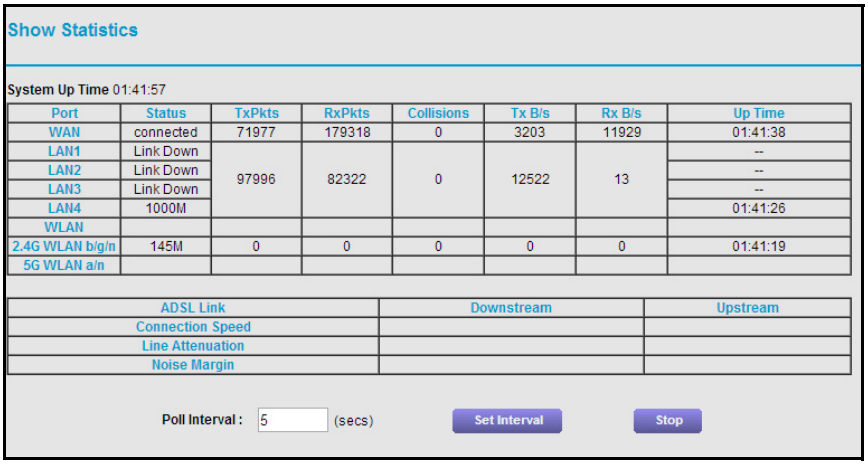
LAN Port.

- **MAC Address**. The Media Access Control address. This is the unique physical address used by the Ethernet (LAN) port of the modem router.
- **IP Address**. The IP address used by the Ethernet (LAN) port of the modem router. The default is 192.168.0.1.
- **DHCP**. Identifies whether the modem router's built-in DHCP server is active for devices on the LAN.

Show Statistics Button

➢ **To view statistics:**

1. Select **ADVANCED Home** or select **Administration > Router Status**.
2. In the Internet Port pane, click the **Show Statistics** button.



The following information is displayed:

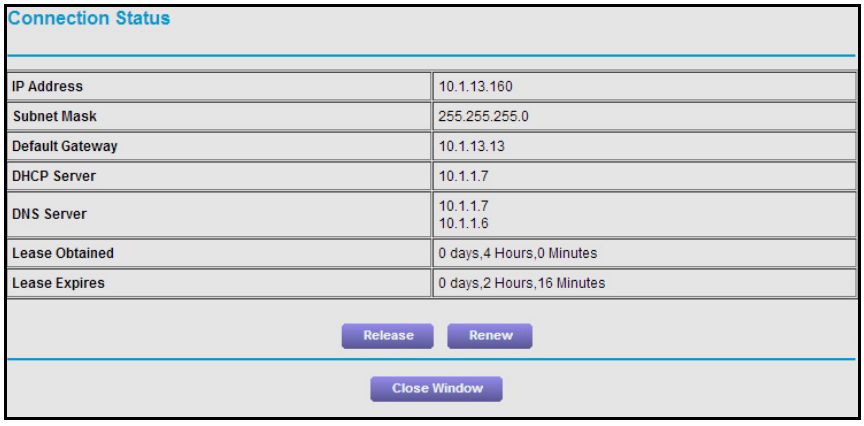
System Up Time. The time elapsed since the modem router was last restarted.

- **Port**. The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:
  - **Status**. The link status of the port.
  - **TxPkts**. The number of packets transmitted on this port since reset or manual clear.
  - **RxPkts**. The number of packets received on this port since reset or manual clear.
  - **Collisions**. The number of collisions on this port since reset or manual clear.
  - **Tx B/s**. The current transmission (outbound) bandwidth used on the WAN and LAN ports.
  - **Rx B/s**. The current reception (inbound) bandwidth used on the WAN and LAN ports.
  - **Up Time**. The time elapsed since this port acquired the link.
- **ADSL Link Downstream or Upstream**. The statistics for the upstream and downstream link. These statistics are of interest to your technical support representative if you have problems obtaining or maintaining a connection.
- **Connection Speed**. Typically, the downstream speed is faster than the upstream speed.
- **Line Attenuation**. The line attenuation increases the farther you are physically located from your ISP's facilities.
- **Noise Margin**. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.
- **Poll Interval**. The interval at which the statistics are updated in this screen. To change the polling frequency, enter a time in seconds in the Poll Interval field and click **Set Interval**. To stop the polling entirely, click **Stop**.

Connection Status Button

➢ **To view the Internet connection status:**

1. Select **ADVANCED Home** or select **Administration > Router Status**.
2. In the Internet Port pane, click the **Connection Status** button.



The following information displays:

- **IP Address**. The IP address that is assigned to the modem router.
- **Subnet Mask**. The subnet mask that is assigned to the modem router.

- **Default Gateway**. The IP address for the default gateway that the wireless modem router communicates with.
- **DHCP Server**. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the wireless modem router.
- **DNS Server**. The IP address of the Domain Name Service server that provides translation of network names to the IP addresses.
- **Lease Obtained**. The date and time when the lease was obtained.
- **Lease Expires**. The date and time that the lease expires.

The Release button returns the status of all the items to 0.

The Renew button refreshes the items.

The Close Window button closes the Connection Status screen.

Wireless Settings (2.4 GHz)

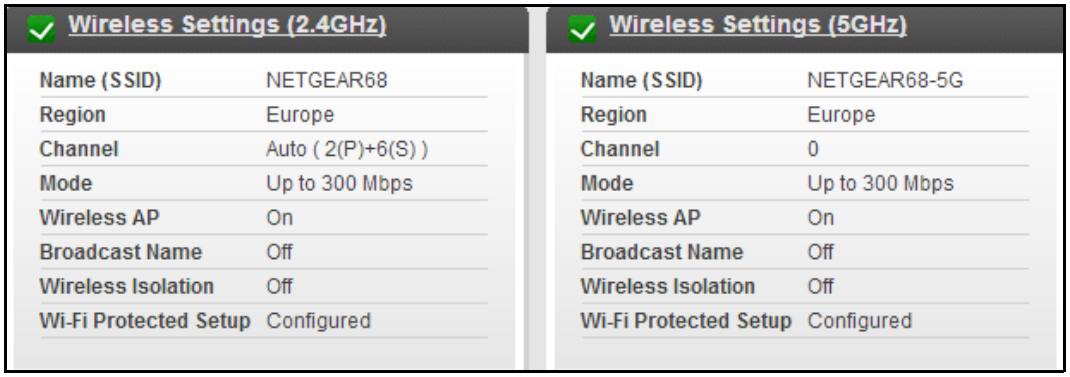


Figure 12. View wireless settings information

The following settings are displayed:

Name (SSID). The wireless network name (SSID) that the modem router uses.

Region. The geographic region where the modem router is being used. It might be illegal to use the wireless features of the modem router in some parts of the world.

Channel. The operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the modem router finds the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 do not interfere with each other.

Mode. The wireless communication mode: Up to 54 Mbps, Up to 217 Mbps (default), and Up to 1300 Mbps.

Wireless AP. Indicates whether the radio feature of the modem router is enabled. If this feature is not enabled, the WiFi LED on the front panel is off.

Broadcast Name. Indicates whether the modem router is broadcasting its SSID.

Wireless Isolation. Wireless isolation prevents wireless clients from communicating with each other when they join the wireless network.

Wi-Fi Protected Setup. Indicates whether WPS is configured for this network.

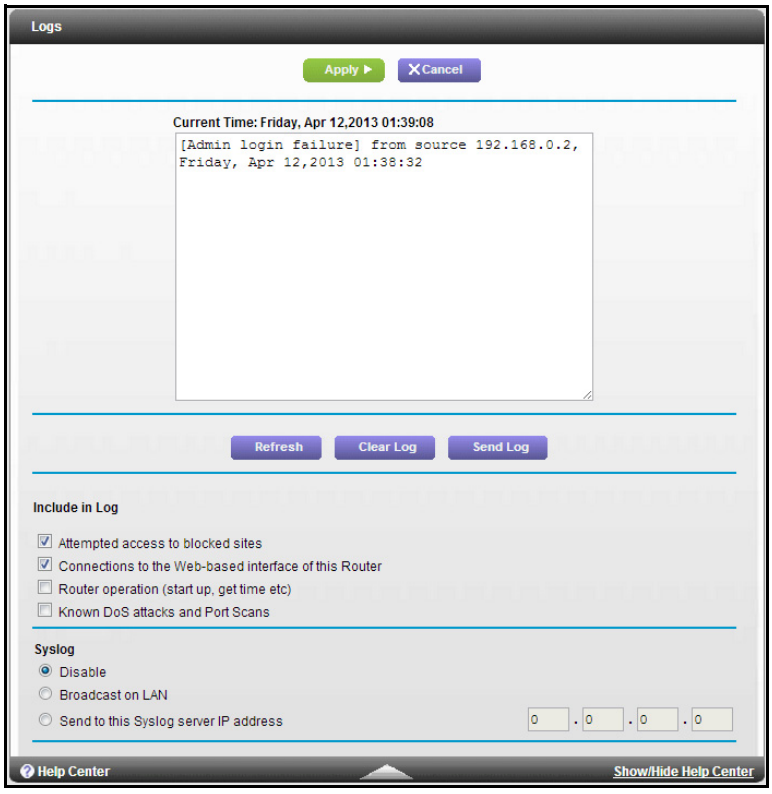
View Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

➢ **To view logs:**

Select **ADVANCED > Administration > Logs**.

The Logs screen displays:



The Logs screen shows the following information:

- **Date and time**. The date and time the log entry was recorded.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Target address**. The name or IP address of the website or news group visited or to which access was attempted.
- **Action**. Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To email the log immediately, click the **Send Log** button.

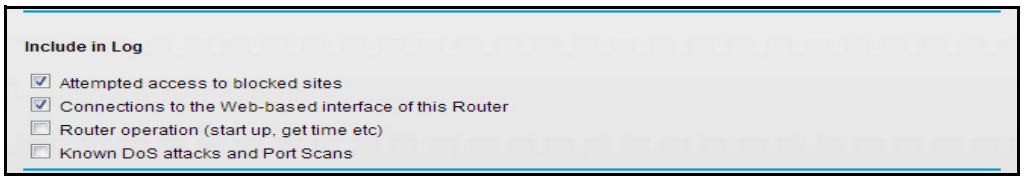
Include in Log

➢ **To include events in the log:**

1. Select **ADVANCED > Administration > Logs**.

   The Logs screen displays.

2. Under Include in Log, select the check box of the events you want to include in the log.



   Selecting all check boxes increases the size of the log, so it is good practice to disable any events that are not really required.

   - **Attempted access to blocked sites**. If selected, attempted Internet accesses that were blocked are logged.
   - **Connections to the Web-based interface of this Router**. If selected, the log tracks each time someone logs in to the router.
   - **Router operation**. If selected, router operations not covered by the preceding selections are logged.
   - **Known DoS attacks and Port Scans**. If selected, denial of service attacks, as well as port scans, are logged.

3. Click **Apply** to save your changes.

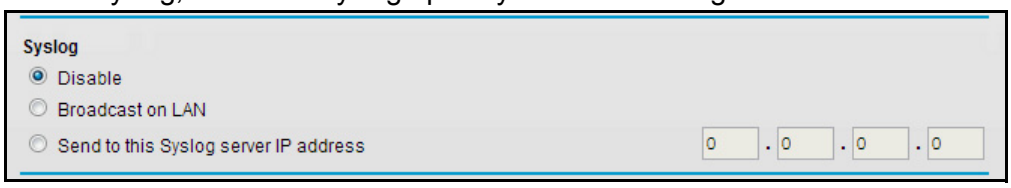
Syslog

➢ **To send logs to a syslog server:**

1. Select **ADVANCED > Administration > Syslog**.

   The Logs screen displays.

2. Under Syslog, select the syslog option you want to configure.



   - **Disable**. Select this if you do not have a syslog server.
   - **Broadcast on LAN**. The syslog data is broadcast rather than sent to a specific syslog server. Use this if your syslog server does not have a fixed IP address.

- **Send to this Syslog server IP address**. If your syslog server has a fixed IP address, select this option, and enter the IP address of your syslog server.

3. Click **Apply** to save your changes.

Manage the Configuration File

The configuration settings of the modem router are stored within the modem router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

➢ **To back up the modem router's configuration settings:**

1. Select **ADVANCED > Administration > Backup Settings**.

2. Click **Back Up**.

   A copy of the current settings is saved.

3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

➢ **To restore configuration settings that you backed up:**

1. Click the **Browse** button to find the cfg file, and select it.
2. Click the **Restore** button.

   The files is uploaded to the modem router.

   The modem router reboots.

WARNING:

Do not interrupt the reboot process.

Erase the Current Configuration Settings

You can use the Erase button erase the configuration and restore the factory default settings. You might want to do this if you move the modem router to a different network or if you changed the password and have forgotten what it is. (The default passwords are on the product label).

You can also use the Restore Factory Settings button on the bottom of the modem router to erase the configuration and restore the factory settings. (See *Factory Settings* on page 149),.

➢ **To erase the configuration settings:**

Click the **Erase** button.

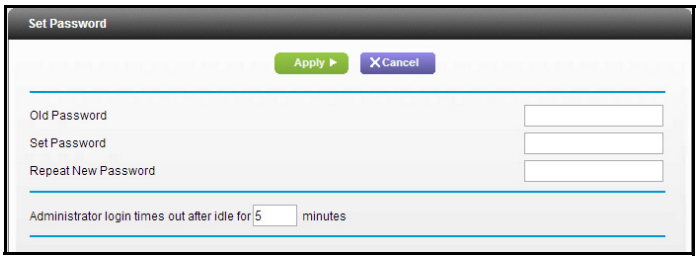
The factory default settings are restored. The user name is admin, the password to password, and the LAN IP address is 192.168.0.1. DHCP is enabled.

Change the Password

This feature let you change the default password that is used to log in to the modem router with the user name **admin**. This is not the same as changing the password for wireless access. The label on the bottom of your modem router shows your unique wireless network name (SSID) and password for wireless access (see *Label* on page 13).

➢ **To set the password for the user name admin:**

1. Select **ADVANCED > Administration > Set Password**.



2. On the Set Password screen, type the old password, and type the new password twice.
3. Change the login time-out to a value between 1 and 99 minutes if the default value of 5 minutes does not meet your needs.
4. Click **Apply**.

   Your changes take effect.

Advanced Settings

8

This chapter describes the advanced features of your modem router. Networking knowledge is needed to implement some of these features.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Distribution System (WDS)*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*

Some selections in the Advanced Setup menu on the Advanced screen are described in separate chapters:

- **Port Forwarding/Port Triggering**. For information about port forwarding and port triggering, see *Chapter 6, Security*.
- **USB Setting**. For more information about the USB Settings screen, see *Specify Approved USB Devices* on page 67.

Advanced Wireless Settings

You can use this screen to turn the wireless radio on and off, to specify WPS settings, to use AP mode, and to set up a wireless access list.

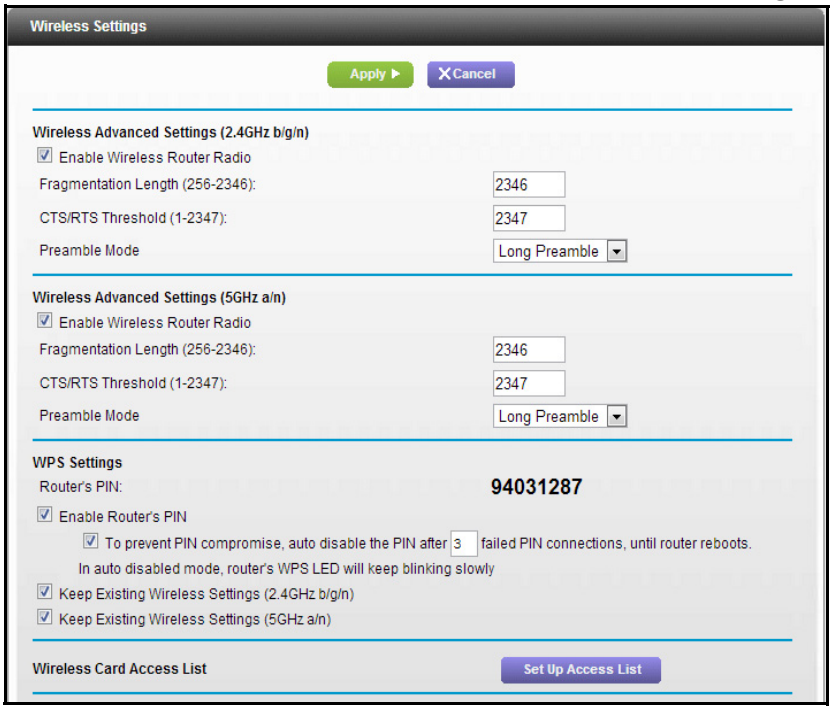
The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options in this screen are reserved for wireless testing and advanced configuration only. Do not change these settings unless you have a specific reason to do so.

Control the Wireless Radio

By default, the wireless radio is enabled so that you can connect wirelessly to the modem router. You can turn the wireless radio on or off in the Advanced Wireless Settings screen or by using the WiFi On/Off button on the modem router front panel. When the wireless radio is off, you can still use an Ethernet cable for a LAN connection to the modem router.

➢ **To turn the wireless radio on or off:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.



   By default, the Enable Wireless Router Radio check box is selected.

2. Select or clear the **Enable Wireless Router Radio** check box.

   If you clear this check box, this turns off the WiFi feature of the wireless modem router.

3. Click **Apply**.

   Your changes take effect.

View or Change WPS Settings

➢ **To specify WPS Settings:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Router's PIN field displays the PIN that you use on a registrar (for example, from the Network Explorer on a Vista Windows computer) to configure the modem router's wireless settings through WPS.

2. (Optional) Select or clear the **Enable Router's Pin** check box.

   By default, the Enable Router's Pin check box is selected. NETGEAR recommends that you leave this check box selected.

3. (Optional) Select or clear the **To prevent PIN compromise** check box.
4. (Optional) Change the number of failed PIN connections in the text field.
5. (Optional) Select or clear the **Keep Existing Wireless Settings** check box.

   By default, the Keep Existing Wireless Settings check box is selected. NETGEAR recommends that you leave this check box selected.

   If you clear this check box, the next time a new wireless client uses WPS to connect to the modem router, the modem router wireless settings change to an automatically generated random SSID and security key.

6. Click **Apply**.

   Your changes are saved.

Set Up a Wireless Access List by MAC Address

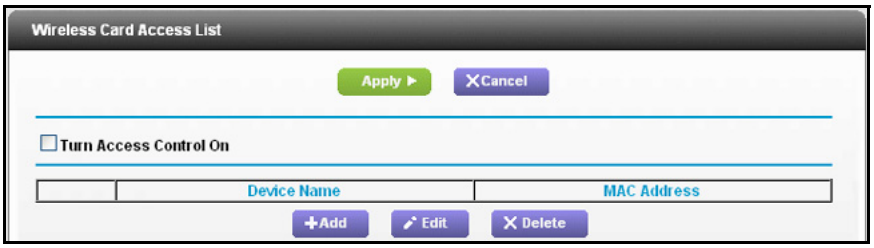
You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses in the Attached Devices screen.

➢ **To restrict access based on MAC addresses:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.
2. Click the **Set Up Access List** button.

   The Wireless Card Access List screen displays.



3. Click **Add**.

   The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

4. If the computer or device you want is in the Available Wireless Cards list, select that radio button; otherwise, type a name and the MAC address.

   You can usually find the MAC address on the bottom of the wireless device.

   You can copy and paste the MAC addresses from the Attached Devices screen into the MAC Address field of this screen. To do this, use each wireless computer to join the wireless network. The computer should then be listed in the Attached Devices screen.

5. Click **Add**.

   The screen changes back to the list screen.

6. Add each computer or device you want to allow to connect wirelessly.
7. Select the **Turn Access Control On** check box.
8. Click **Apply**.

➢ **To edit a wireless device or delete it from the access list:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Advanced Wireless Settings screen displays.

2. In the table, select the radio button next to the wireless device that you want to edit or delete.
3. Do one of the following:
   - Click the **Edit** button.

     The Edit Wireless Card screen displays.

     a. Edit the address information.
     b. Click the **Accept** button.
   - Click the **Delete** button.

   The address is removed from the table.

Wireless Distribution System (WDS)

You can set up the modem router to be used as a wireless access point (AP). Doing this enables the modem router to act as a wireless repeater. A wireless repeater connects to another wireless modem router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of wireless distribution system (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

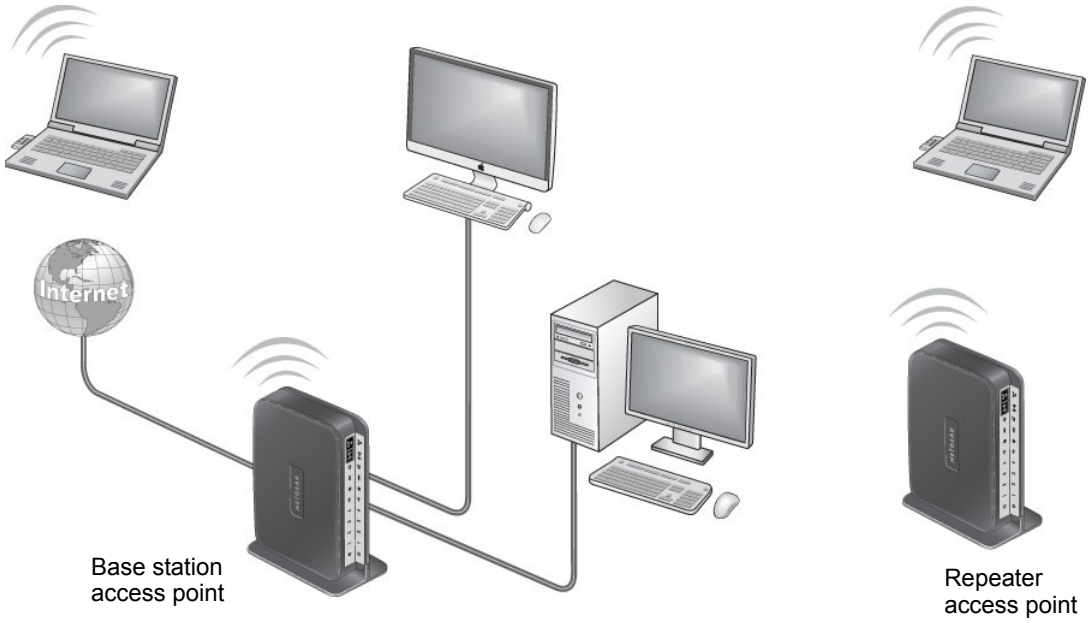


Figure 13. Wireless repeating scenario

Note: To use the wireless repeating function, you need to select None as the security option in the Wireless Setup screen, and you cannot select Auto Channel. For more information, see *Basic Wireless Setup* on page 30.

Wireless base station. The modem router acts as the parent access point, that bridges traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you have to know the MAC address of the child repeater access point. Often, the MAC address is on the product label.

Wireless repeater. The modem router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

The modem router is always in dual-band concurrent mode, unless you turn off one radio. If you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless modem router or wireless base station, dual-band concurrent mode is not affected.

For you to set up a wireless network with WDS, both access points have to meet the following conditions:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all of the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

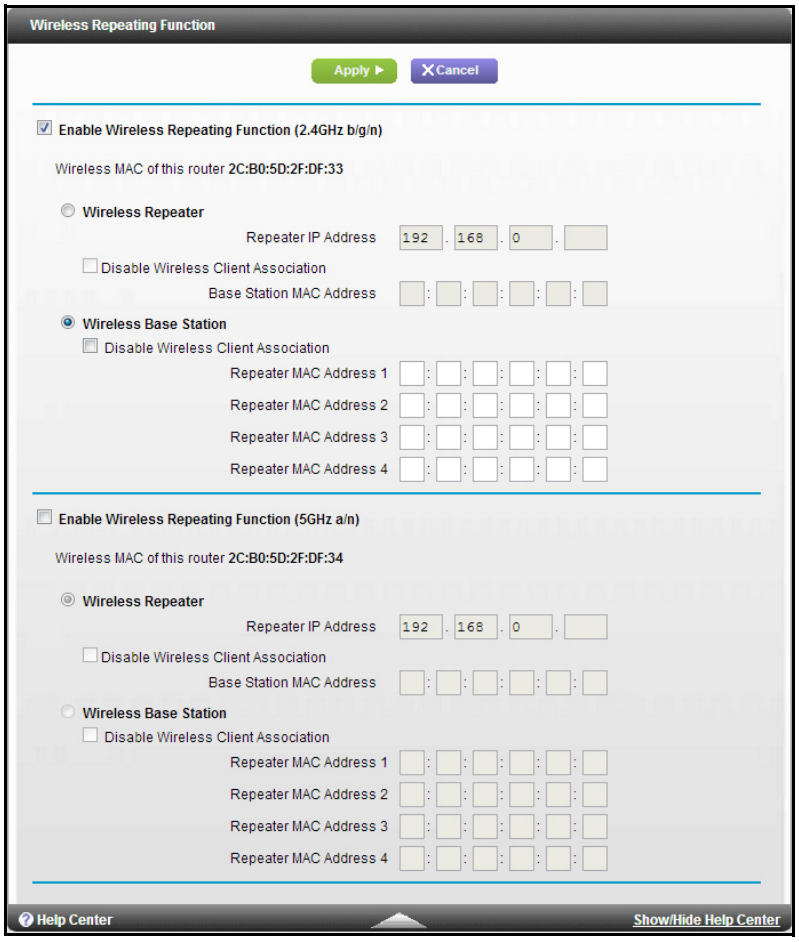
Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

➢ **To set up the base station:**

1. Set up both units with the same wireless settings (SSID, mode, channel, and security). The wireless security option has to be set to **None** or **WEP**.
2. Select **ADVANCED > Advanced Setup > Wireless Repeating**.
3. Select the **Enable Wireless Repeating Function** check box.

4. Select the **Wireless Base Station** radio button.



5. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the base station and allowing LAN client associations only.

   You can leave the check box cleared if you prefer wireless clients to be able to associate with the base stations.

6. In the Repeater MAC Address 1 through 4 fields, enter the MAC addresses for the access points that should function as repeaters.

   If your modem router is the base station, it can function as the “parent” for up to four other access points.

7. Click the **Apply** button.

   Your changes are saved.

Set Up a Repeater

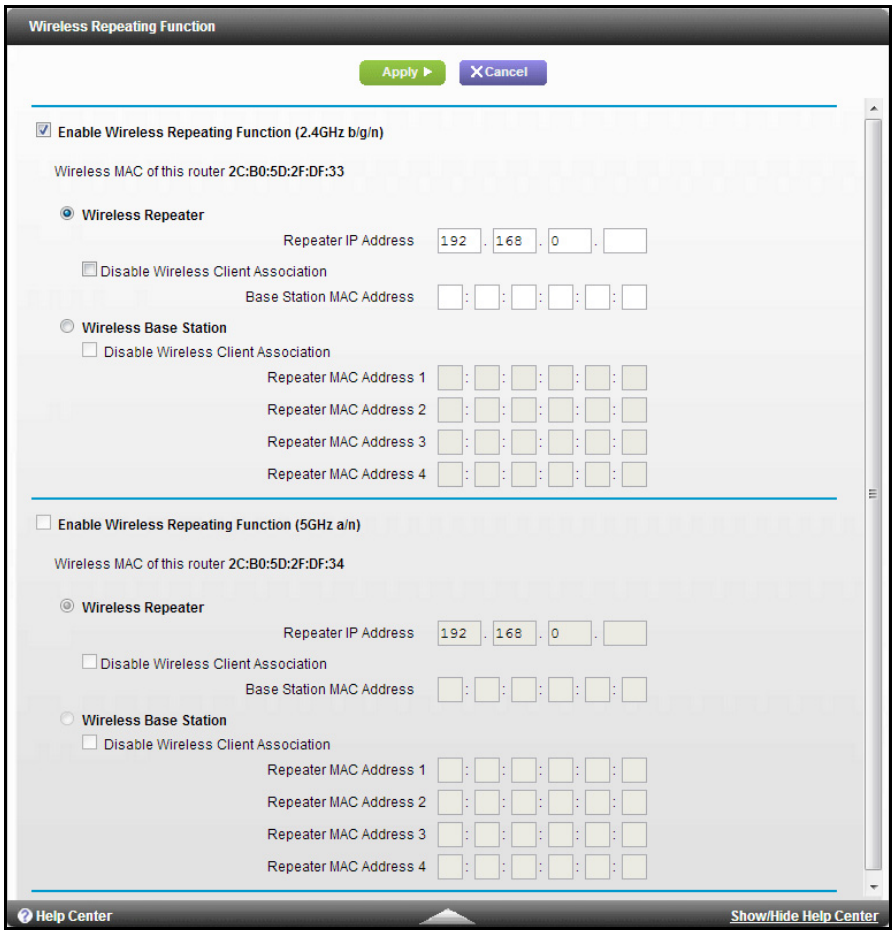
Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

If you are using the modem router as the base station with a non-NETGEAR router as the repeater, you might need to change more configuration settings. In particular, you should disable the DHCP server function on the access point that is the repeater.

➤ **To configure the modem router as a repeater:**

1. Log in to the modem router that will be the repeater.
2. Select **BASIC > Wireless** and verify that the wireless settings match the base unit exactly.

   The wireless security option has to be set to **WEP** or **None**.
3. Select **ADVANCED > Advanced Setup > Wireless Repeating**.
4. Select the **Enable Wireless Repeating Function** check box.
5. Select the **Wireless Repeater** radio button.



6. Fill in the Repeater IP Address field.

   This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.
7. (Optional) Select the Disable
8. In the Base Station MAC Address field, enter the MAC address for your modem router.
9. Click **Apply**.

Your changes are saved.

10. Verify connectivity across the LANs.

    A computer on any wireless or wired LAN segment of the modem router can connect to the Internet or share files and printers with any other computer or server connected to the other access point.

Set Up a Point-to-Point Bridge

In point-to-point bridge mode, the modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled. Only wired clients can be connected. Use wireless security to protect this communication. The following figure shows an example of point-to-point bridge mode.

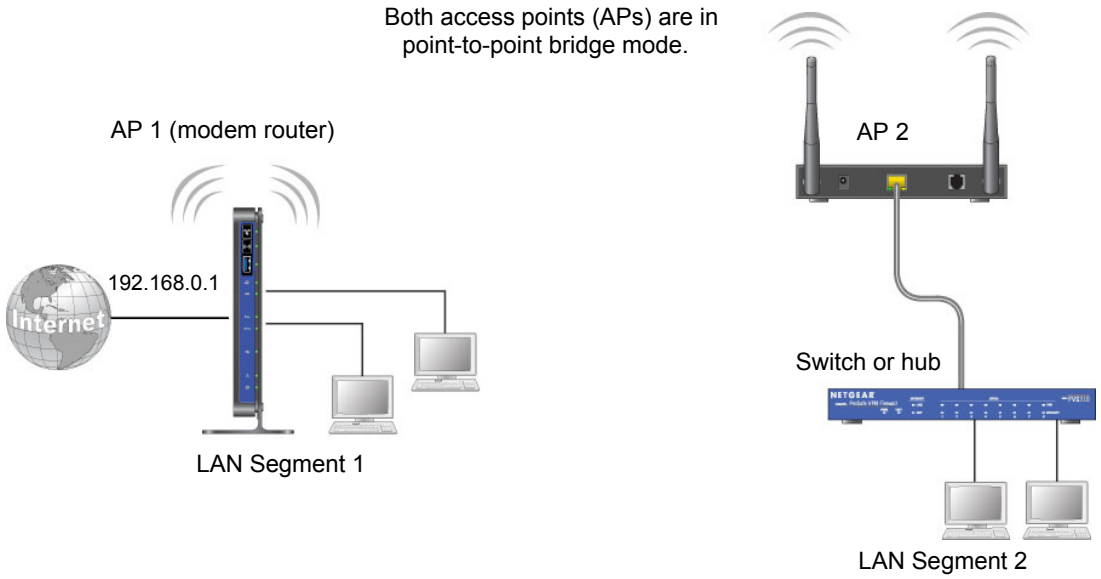


Figure 14. Point-to-point bridge example

➢ **To set up a point-to-point bridge configuration:**

1. Set up your modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.
   a. In the Wireless Repeating Function screen, select the **Enable Wireless Repeating Function** check box.
   b. Select either the **Wireless Repeater** or **Wireless Base Station** radio button.
   c. Select the corresponding **Disable Wireless Client Association** check box.
   d. Enter the MAC address for the other access point in the bridge.

      Depending on your selection in step a, use either the Base Station MAC Address field or the Repeater MAC Address 1 field.

   e. Click **Apply**.
2. Set up the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

If your modem router is the repeater, then set up AP 2 as the base station; otherwise, set up AP 2 as the repeater.

3. Set up both access points and verify that they use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.
4. Disable the DHCP server on AP 2. AP 1 will then be the DHCP server.
5. Verify connectivity across LAN Segment 1 and LAN Segment 2.

   A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

Set Up a Multi-Point Bridge

Multi-point bridge mode allows a router to bridge to multiple peer access points simultaneously. Wireless client associations are disabled. Only wired clients can be connected.

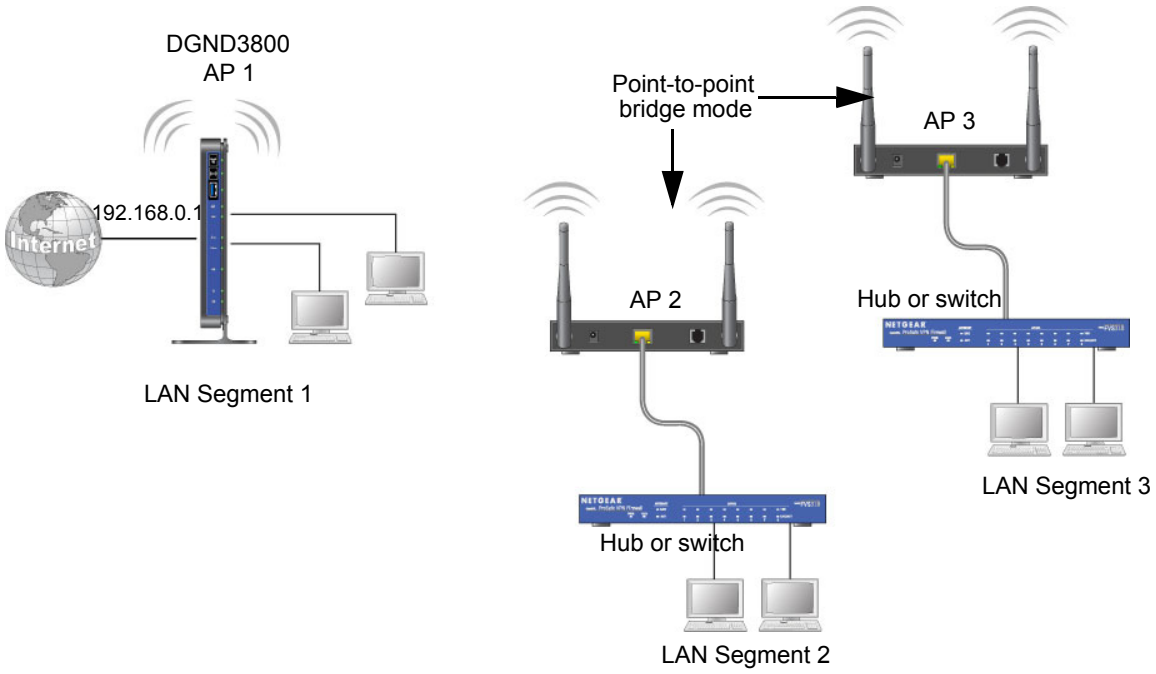


Figure 15. Multi-point bridge example

Multi-point bridge mode configuration includes the following steps:

- Set up the modem router for wireless repeating as the base station, and specify the MAC addresses of the access points that are repeaters.
- Set up the other access points for wireless repeating as repeaters, and specify the MAC address of the modem router as the base station.
- Use wireless security to protect this traffic.

➢ **To set up the multi-point bridge configuration:**

In this example, the modem router is AP 1 on LAN Segment 1 because it is in a central location.

1. Set up your modem router to be the base station in the bridge.
   a. In the Wireless Repeating Function screen for your modem router, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Base Station** radio button.
   c. Select the corresponding **Disable Wireless Client Association** check box.
   d. Enter the MAC address for the other access points in the bridge in the Repeater MAC Address 1 and Repeater MAC Address 2 fields.
   e. Click **Apply**.
2. Set up AP 2 and AP 3 to be wireless repeaters.
   a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Repeater** radio button.
   c. Select the corresponding **Disable Wireless Client Association** check box.
   d. Enter the MAC addresses for your modem router in the Base Station MAC Address field.
   e. Click **Apply**.
3. Disable the DHCP server on AP 2 and AP 3. AP 1 will then be the DHCP server.
4. Verify the following for all access points:
   - The modem router and other access points operate in the same LAN network address range as the LAN devices.
   - Only one access point, your modem router in *Figure 15* on page 103, is set up as the base station. The others are set up as repeaters.
   - All access points, including your modem router, are on the same LAN. That is, all the access point LAN IP addresses are in the same network.
   - If you are using DHCP, all access points should be set as DHCP clients. This setting is **Obtain an IP address automatically (DHCP Client)** in the Basic Settings screen.
   - All access points, including your modem router, use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.
5. Verify connectivity across the LANs.

   A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other computers or servers connected to any of the three LAN segments.

Note: Wireless stations configured as in *Figure 14* on page 102 cannot connect to the modem router or access points. If you want wireless stations to access any LAN segment, use additional access points in any LAN segment.

Repeater with Wireless Client Association

In the repeater mode with wireless client association, your modem router sends all traffic to a base station access point. You can set up the modem router as either the base station (parent) or as the repeater (child) access point.

Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this modem router.
- You cannot configure a sequence of parent-child APs. You are limited to only one parent access point, although if your modem router is the parent access point, it can connect with up to four child access points.

The following figure shows an example of a repeater mode configuration.

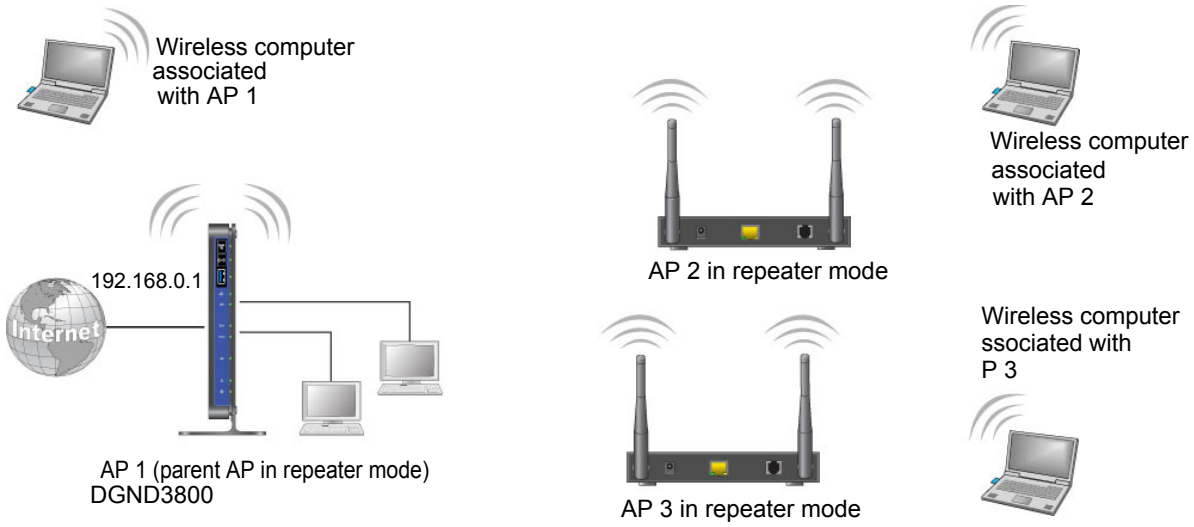


Figure 16. Repeater example

➢ **To set up a repeater with wireless client association:**

In this example, the modem router is the base station, but you can set it up to be the repeater with another AP as the base station if you want.

1. Set up your modem router to be the base station.
   a. In the Wireless Repeating Function screen for your modem router, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Base Station** radio button.

c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).

d. Enter the MAC addresses for AP 2 and AP 3 in the Repeater MAC Address 1 and Repeater MAC Address 2 fields.

e. Click **Apply**.

2. Set up AP 2 and AP 3 to be wireless repeaters.

a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.

b. Select the **Wireless Repeater** radio button.

c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).

d. Enter the MAC addresses for your modem router in the Base Station MAC Address field.

e. Click **Apply**.

3. Verify the following for all access points:

- Each access point operates in the same LAN network address range as the LAN devices.
- The access points are on the same LAN. That is, the LAN IP addresses for the access points are in the same network.
- If you are using DHCP, access point devices are set to **Obtain an IP address automatically (DHCP Client)** in the Basic Settings screen.
- Access point devices use the same SSID, channel, authentication mode, and encryption.

Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other computers or servers connected to any of the three WLAN segments.

Dynamic DNS

If your ISP assigned you a fixed IP address, you can register a domain name and link it to your IP address by public DNS. However, most Internet accounts use dynamically assigned IP addresses that can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

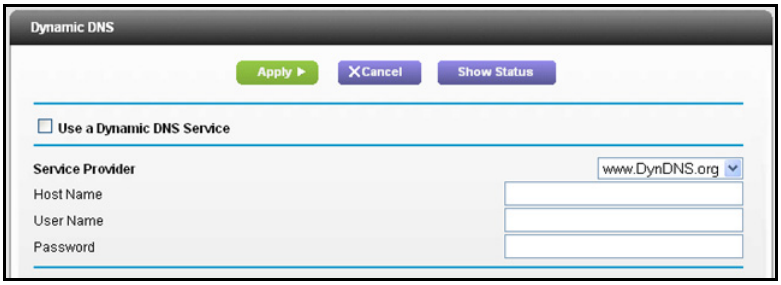
If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Your modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at *http://www.dyndns.org* and obtain an account and host name that you configure in the modem router. Then, whenever your ISP-assigned IP address changes, your modem router automatically contacts the Dynamic DNS service

provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your modem router at http://hostname.dyndns.org.

➢ **To set up Dynamic DNS:**

1. Select **ADVANCED > Advanced Setup > Dynamic DNS**.



2. Register for an account with one of the Dynamic DNS service providers whose URLs are in the Service Provider list.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the URL of your Dynamic DNS service provider.

   For example, for DynDNS.org, select **www.DynDNS.org**.
5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
6. Type the user name for your Dynamic DNS account.

   This is the name that you use to log in to your account, not your host name.
7. Type the password (or key) for your Dynamic DNS account.
8. Click **Apply**.

   Your changes are saved.

Static Routes

Static routes provide more routing information to your modem router. Typically, you do not need to add static routes. You have to configure static routes only for unusual cases such as multiple modem routers or multiple IP subnets on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN modem router on your home network for connecting to the company where you are employed. This modem router's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

When you first configured your modem router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem router forwards your

request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

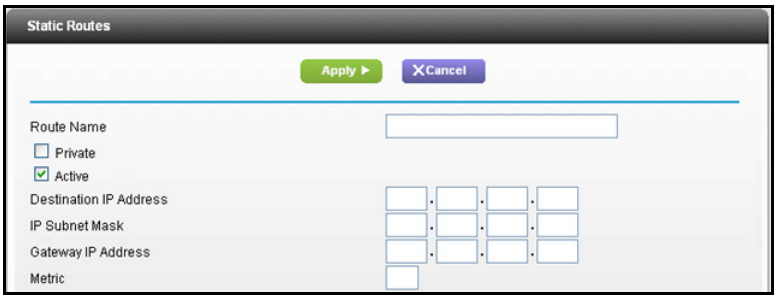
In this case you have to define a static route, telling your modem router that 134.177.0.0 should be accessed through the ISDN modem router at 192.168.0.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN modem router at 192.168.0.100.
- A metric value of 1 works because the ISDN modem router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

➢ **To set up a static route:**

1. Select **ADVANCED > Advanced Setup > Static Routes**.
2. Click **Add.**

   The Static Routes screen displays.



3. In the Route Name field, type a name for this static route (for identification purposes only).
4. Select the **Private** check box if you want to limit access to the LAN only.

   If Private is selected, the static route is not reported in RIP.
5. Select the **Active** check box to make this route effective.
6. Type the IP address of the final destination.
7. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
8. Type the gateway IP address, which has to be on the same LAN segment as the modem router.
9. Type a number from 1 through 15 as the metric value.

   This value represents the number of modem routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
10. Click **Apply.**

    The static route is added.

➢ **To edit or delete a static route:**

1. Select **ADVANCED > Advanced Setup > Static Routes**.

   The Static Routes screen displays.

2. In the table, select the radio button next to the route that you want to edit or delete.
3. Do one of the following:
   - Click the **Edit** button.

     The Static Routes screen adjusts.

     a. Edit the route information.

     b. Click the **Apply** button.
   - Click the **Delete** button.

     The route is removed from the table.

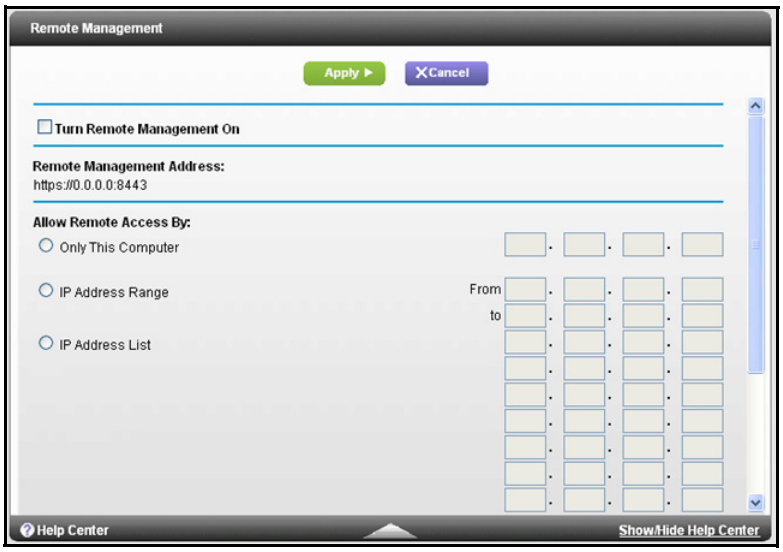
Remote Management

The remote management feature lets you upgrade or check the status of your modem router over the Internet.

Note: Be sure to change the modem router default login password to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

➢ **To set up remote management:**

1. Select **ADVANCED > Advanced Setup > Remote Management**.



2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the modem router's remote management.

   For enhanced security, restrict access to as few external IP addresses as practical.

   - To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
   - To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
   - To specify IP addresses, select **IP Address List** and type the allowed IP addresses.
   - To allow access from any IP address on the Internet, select **Everyone**.
4. Specify the port number for accessing the web management interface.

   Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
5. Click **Apply**.

   Your changes take effect.
6. When you access your modem router from the Internet, type your modem router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.

   For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

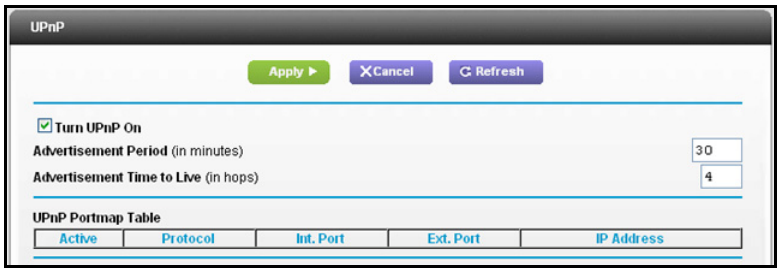
Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➢ **To turn on Universal Plug and Play:**

1. Select **ADVANCED > Advanced Setup > UPnP**.



2. Select the **Turn UPnP On** check box.

   By default, this check box is selected. UPnP for automatic device configuration can be enabled or disabled. If the Turn UPnP On check box is cleared, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.

3. Type the advertisement period in minutes.

   The advertisement period specifies how often the modem router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

4. Type the advertisement time to live in hops.

   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

5. Click the **Apply** button.

   The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the modem router. The UPnP Portmap Table also shows which ports are open, what type of ports are open, and whether each open port is still active for each IP address.

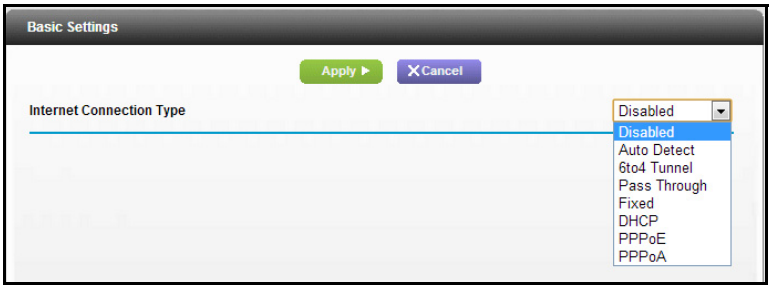
To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

IPv6

You can use this feature to set up an IPv6 Internet connection type if genie does not detect it automatically.

➢ **To set up an IPv6 Internet connection type:**

1. Select **Advanced > Advanced Setup > IPv6**.



2. In the Internet Connection Type list, select the IPv6 connection type.

   Your Internet service provider (ISP) can provide this information.

   - If you are not sure, select **Auto Detect** so that the modem router detects the IPv6 type that is in use.
   - If your Internet connection does not use PPPoE, DHCP, or fixed, but is IPv6, select **Auto Config**.

   For more information about Internet connection types, see the following sections.

3. Click **Apply**.

   Your changes take effect.

Requirements for Entering IPv6 Addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

Auto Detect

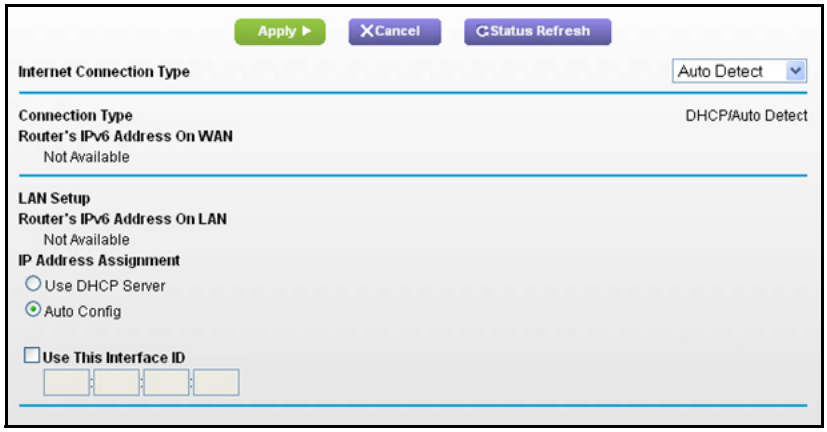
➢ **To set up an IPv6 Internet connection through auto detection:**

1. Select **ADVANCED > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **Auto Detect**.

   The screen adjusts:



   The modem router automatically detects the information in the following fields:

   - **Connection Type**. This field indicates the connection type that is detected.
   - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
   - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
   - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
   - **Auto Config**. This is the default setting.
4. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

   If you do not specify an ID here, the modem router generates one automatically from its MAC address.

5. Click the **Apply** button.

IPv6 6to4 Tunnel

The remote relay router is the router to which your modem router creates the 6to4 tunnel. Make sure that the IPv4 Internet connection is working before you apply the 6to4 tunnel settings for the IPv6 connection.

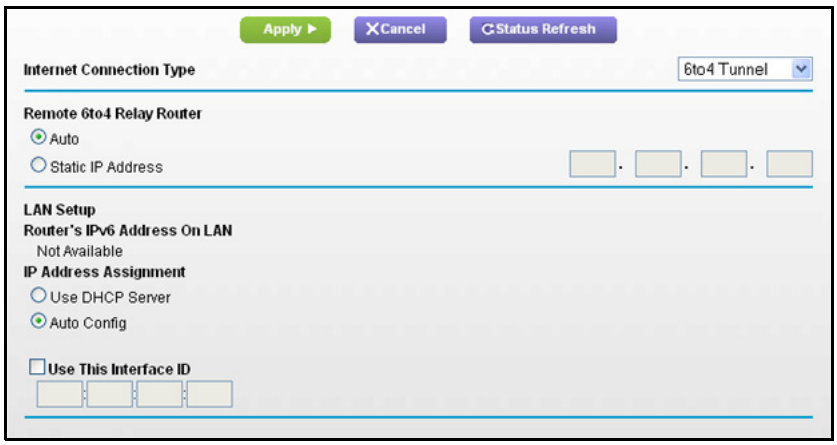
➢ **To set up an IPv6 Internet connection by using a 6to4 tunnel:**

1. Select **ADVANCED > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **6to4 Tunnel**.

   The screen adjusts:



   The modem router automatically detects the information in the following fields:

   - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
   - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. Configure the remote 6to4 relay modem router settings by selecting one of the following buttons:
   - **Auto**. Your modem router uses any remote relay router that is available on the Internet. This is the default setting.
   - **Static IP Address**. Enter the static IPv4 address of the remote relay router. This address is usually provided by your IPv6 ISP.
4. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
   - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.

- **Auto Config**. This is the default setting.

5. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

   If you do not specify an ID here, the modem router generates one automatically from its MAC address.

6. Click the **Apply** button.

IPv6 Pass Through

In pass-through mode, the modem router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The modem router does not process any IPv6 header packets.

➢ **To set up a pass-through IPv6 Internet connection:**

1. Select **ADVANCED > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **Pass Through**.

   The screen adjusts, but no additional fields display.

3. Click the **Apply** button.

IPv6 Fixed

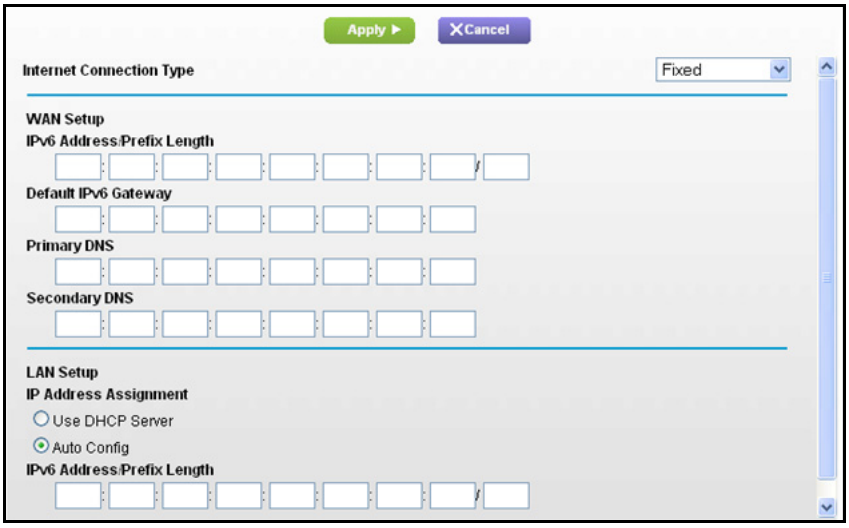
➢ **To set up a pass-through IPv6 Internet connection:**

1. Select **ADVANCED > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **Fixed**.

The screen adjusts:



3. Configure the fixed IPv6 addresses for the WAN connection:
   - **IPv6 Address/Prefix Length**. The IPv6 address and prefix length of the modem router WAN interface.
   - **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway, which should be on the modem router's WAN interface.
   - **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the modem router.
   - **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the modem router.

   Note: *If you do not specify the DNS servers, the modem router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup screen. (See Internet Setup on page 26.)*

4. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
   - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
   - **Auto Config**. This is the default setting.
5. In the IPv6 Address/Prefix Length fields, specify the static IPv6 address and prefix length of the modem router's LAN interface.

   If you do not specify an ID here, the modem router generates one automatically from its MAC address.
6. Click the **Apply** button.

IPv6 DHCP

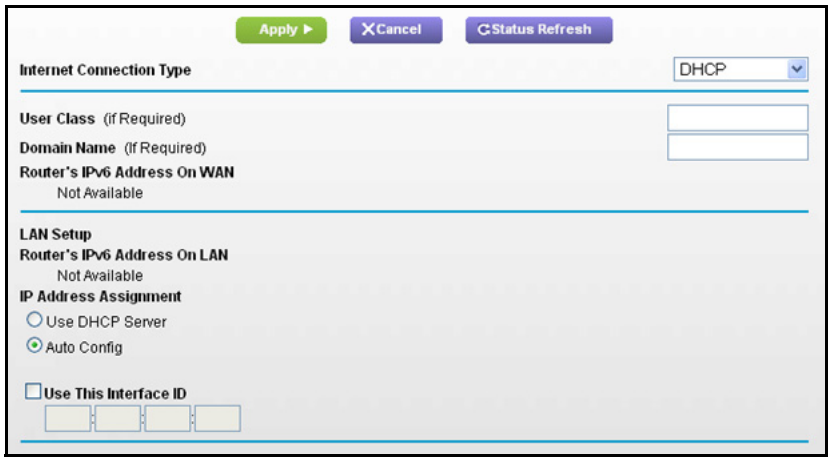
➢ **To set up an IPv6 Internet connection with a DHCP server:**

1. Select **ADVNCED > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **DHCP**.

   The screen adjusts:



   The modem router automatically detects the information in the following fields:

   - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
   - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. (Optional) In the DHCP User Class (If Required) field, enter a host name.

   Most people do not need to fill in this field, but if your ISP has given you a specific host name, enter it here.

4. (Optional) In the Domain Name (If Required) field, enter a domain name.

   You can type the domain name of your IPv6 ISP. (Do not enter the domain name for the IPv4 ISP here.) For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)

5. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

- **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
- **Auto Config**. This is the default setting.

6. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

   If you do not specify an ID here, the modem router generates one automatically from its MAC address.

7. Click the **Apply** button.

IPv6 PPPoE

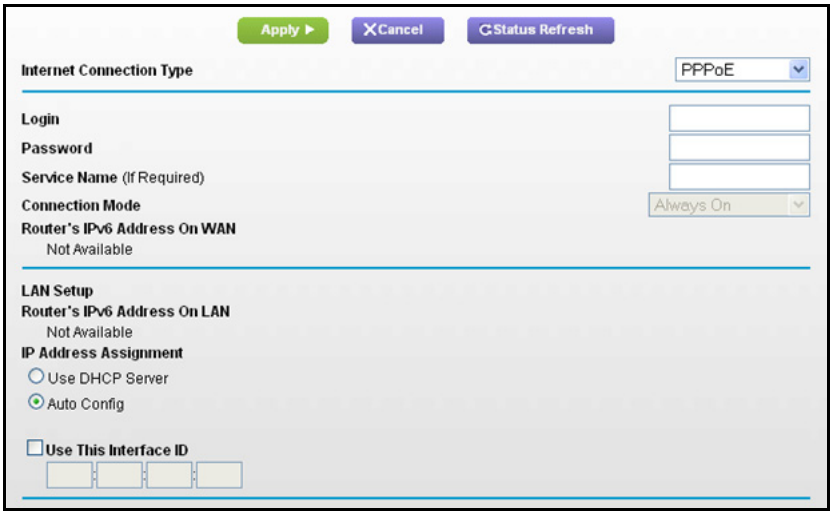
➢ **To set up a PPPoE IPv6 Internet connection:**

1. Select **ADVANCED > Advanced Setup > IPv6**.

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **PPPoE**.

   The screen adjusts:



   The modem router automatically detects the information in the following fields:

   - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
   - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. In the Login fields, enter the login information for the ISP connection.

This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, then you would type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.

4. In the Password field, enter the password for the ISP connection.
5. In the Service Name name field, enter a service name.

   If your ISP did not provide a service name, leave this field blank.

   Note: *The default setting of the Connection Mode field is Always on to provide a steady IPv6 connection. The modem router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the modem router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.*

6. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
   - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
   - **Auto Config**. This is the default setting.
7. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

   If you do not specify an ID here, the modem router generates one automatically from its MAC address.
8. Click the **Apply** button.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic that passes through the modem router Internet port. You can set limits for traffic volume.

➢ **To monitor Internet traffic:**

1. Click **ADVANCED > Advanced Setup > Traffic Meter**.

Scroll to view more settings

2. Select the **Enable Traffic Meter** check box.
3. (Optional) Control the volume of Internet traffic.

   You can use either the traffic volume control feature or the connection time control feature to do this.

   - Select the **Traffic volume control by** radio button and then select one of the following options:
     - **No Limit**. No restriction is applied when the traffic limit is reached.
     - **Download only**. The restriction is applied to incoming traffic only.
     - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
   - Select the **Connection time control** radio button and enter the allowed hours in the Monthly limit field.
4. (Optional) If your ISP charges an amount of extra data volume when you make a new connection, enter the extra data volume in MB in the Round up data volume for each connection by field.
5. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

   If you want the traffic counter to start immediately, click the **Restart Counter Now** button.
6. In the Traffic Control section, specify whether the modem router should issue a warning message before the monthly limit of Mbytes or hours is reached.

   By default, the value is 0 and no warning message is issued. You can select one of the following to occur when the limit is attained:

   - The Internet LED blinks green or amber.
   - The Internet connection is disconnected and disabled.
7. Click the **Apply** button.

The Internet Traffic Statistics section helps you to monitor the data traffic.

Click the **Refresh** button to update the Traffic Statistics section.

Click the **Traffic Status** button to display more information about the data traffic on your modem router and to change the poll interval.

Virtual Private Networking

9

This chapter describes how to use the virtual private networking (VPN) features of the modem router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

This chapter contains the following sections:

- *Overview of VPN Configuration*
- *Set Up a Client-to-Gateway VPN*
- *Add a Gateway-to-Gateway VPN Tunnel*
- *Activate a VPN Tunnel*
- *View or Change the Status of a VPN Tunnel*
- *Auto Policy Example*
- *Add or Edit a VPN Auto Policy*
- *Add or Edit a Manual VPN Policy*

Overview of VPN Configuration

The modem router supports both client-to-gateway and gateway-to-gateway VPN tunnels. The modem router supports up to five concurrent tunnels.

Client-to-Gateway VPN Tunnels

Client-to-gateway VPN tunnels provide secure access from a remote computer, such as a telecommuter connecting to an office network.

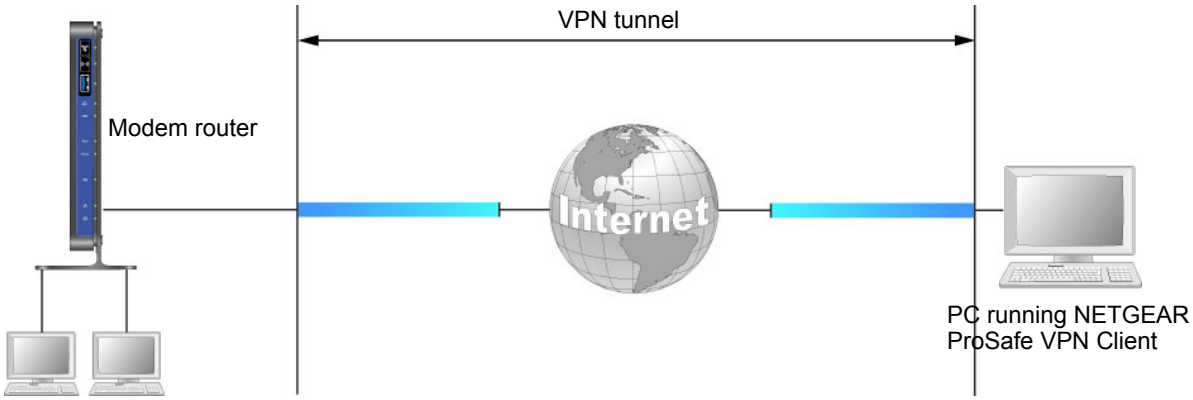


Figure 17. Telecommuter VPN tunnel

A VPN client access allows a remote computer to connect to your network from any location on the Internet. The remote computer is one tunnel endpoint, running the VPN client software. The modem router on your network is the other tunnel endpoint. For more information about how to set up this configuration, see *Set Up a Client-to-Gateway VPN* on page 124.

Gateway-to-Gateway VPN Tunnels

Gateway-to-gateway VPN tunnels provide secure access between networks, such as a branch or home office and a main office.

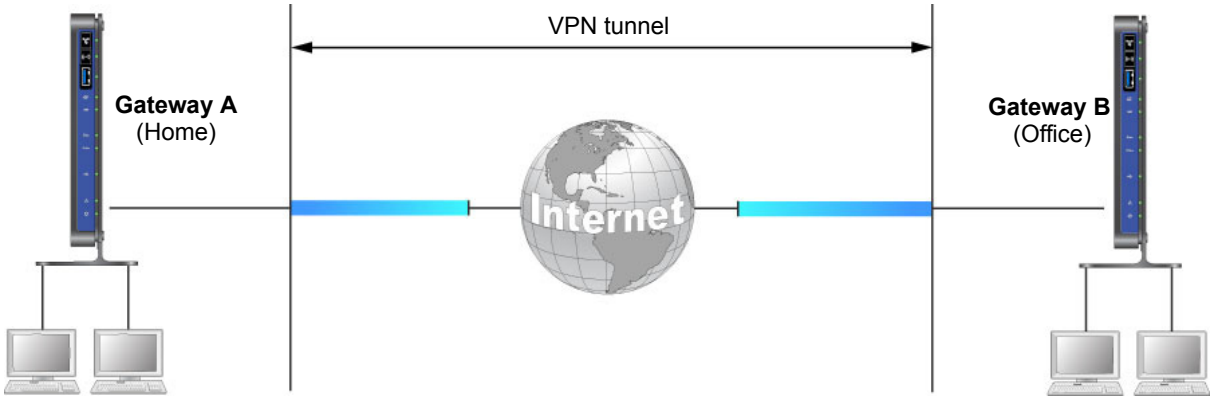


Figure 18. VPN tunnel between networks

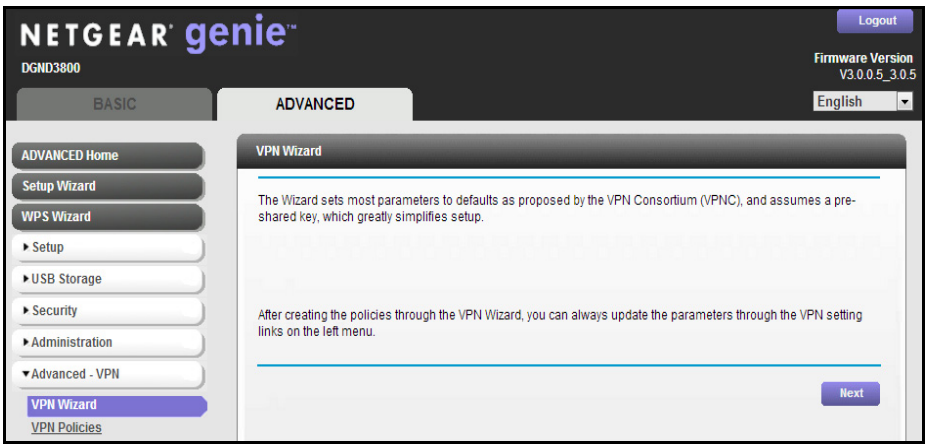
A VPN tunnel between gateways is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use gateways on each end of the tunnel to form the VPN tunnel endpoints. For more information about how to set up this configuration, see *Add a Gateway-to-Gateway VPN Tunnel* on page 125.

Set Up a Client-to-Gateway VPN

This section describes using the VPN Wizard to set up the VPN tunnel. If you want to manually specify the settings, see *Auto Policy Example* on page 131.

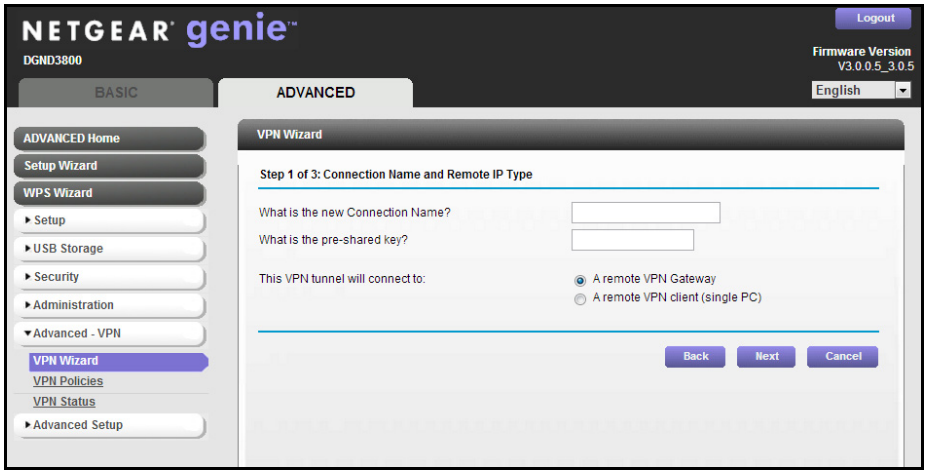
➢ **To configure a client-to-gateway VPN tunnel:**

1. Select **ADVANCED > Advanced - VPN > VPN Wizard**.



2. Click **Next**.

   The following screen displays:

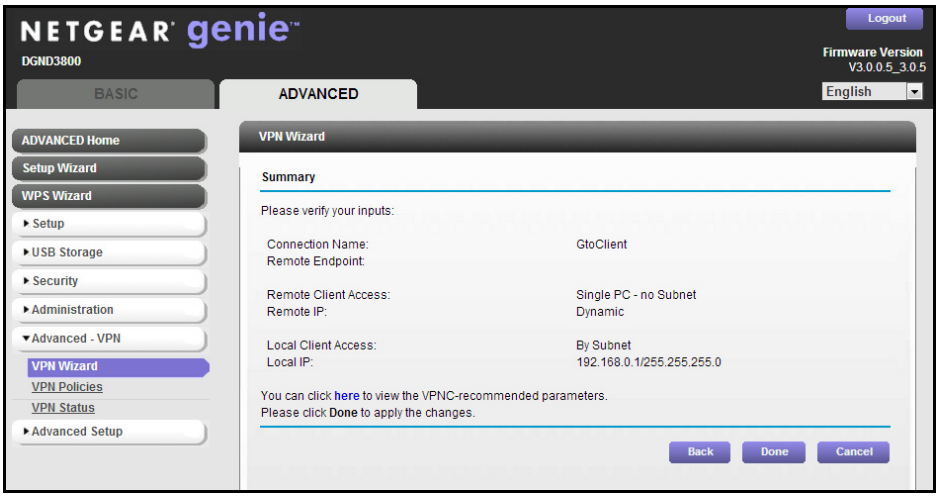


3. Fill in the Connection Name and pre-shared key fields.

   The connection name is for convenience and does not affect how the VPN tunnel functions.

4. Select **A remote VPN client (single PC)** radio button and click **Next**.

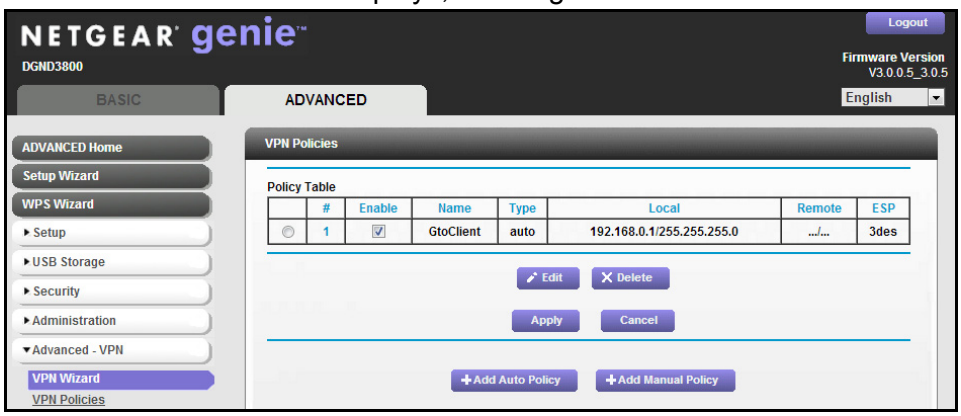
   The Summary screen displays:



   Note: *To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the* ***here*** *link.*

5. Click **Done**.

   The VPN Policies screen displays, showing that the new tunnel is enabled:



6. (Optional) To view or modify a tunnel's settings, select its radio button and click **Edit**.
7. Use VPN client software on the computer to configure it as a VPN client.

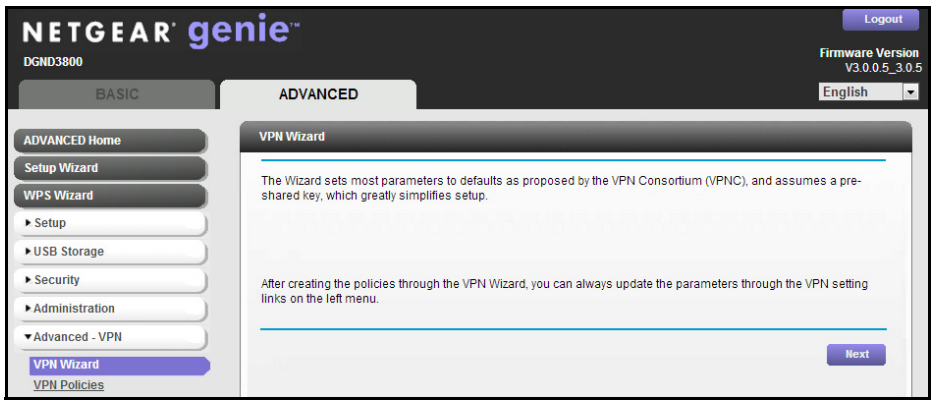
Add a Gateway-to-Gateway VPN Tunnel

This section describes how to use the VPN Wizard to set up the VPN tunnel between two gateways. The LAN IP address ranges of each VPN endpoint have to be different. The connection will fail if both are using the default address range of 192.168.0.x.

➢ **To add a gateway-to-gateway VPN tunnel:**

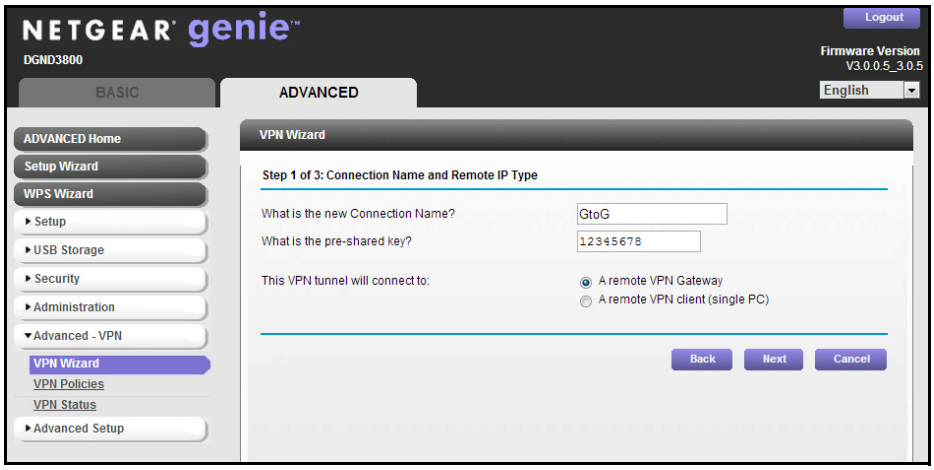
1. Log in to Gateway A on LAN A.

2. Select **ADVANCED > Advanced - VPN > VPN Wizard**.



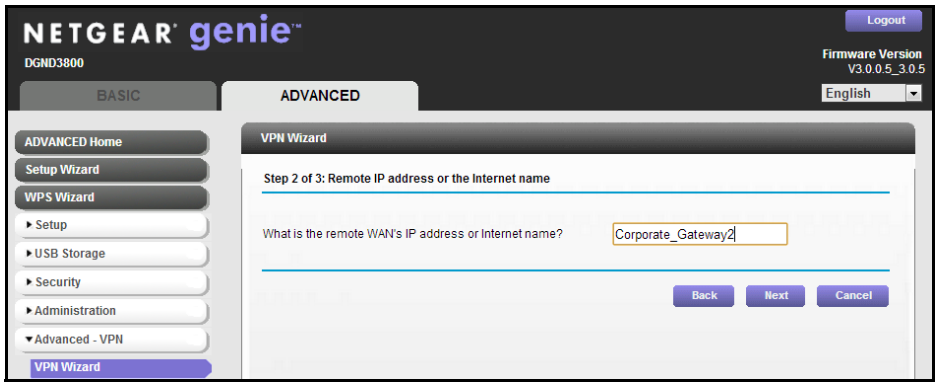
3. Click **Next**.

   The following screen displays:



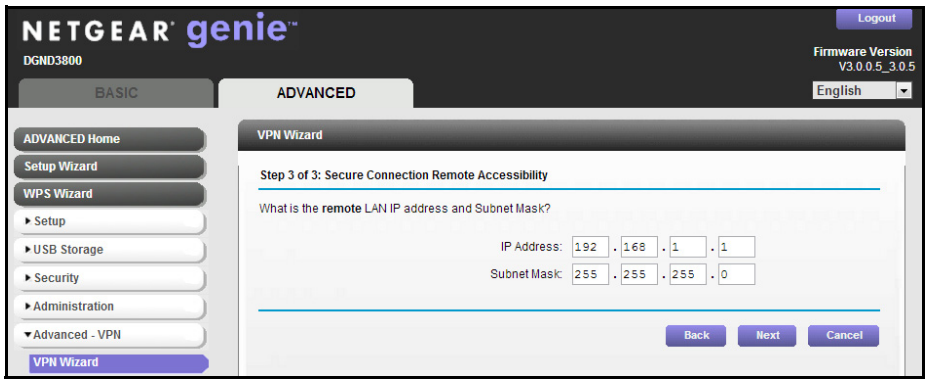
4. Fill in the Connection Name and pre-shared key fields.
5. Select the **A remote VPN Gateway** radio button and click **Next**.

   The following screen displays:



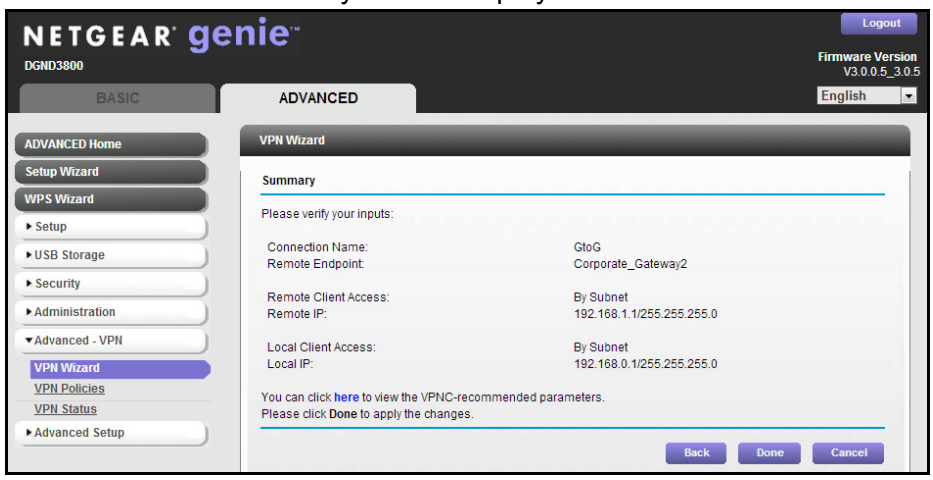
6. Fill in the IP address or FQDN for the target VPN endpoint WAN connection, and click **Next**.

The following screen displays:



7. Fill in the IP Address and Subnet Mask fields for the target endpoint that can use this tunnel, and click **Next**.

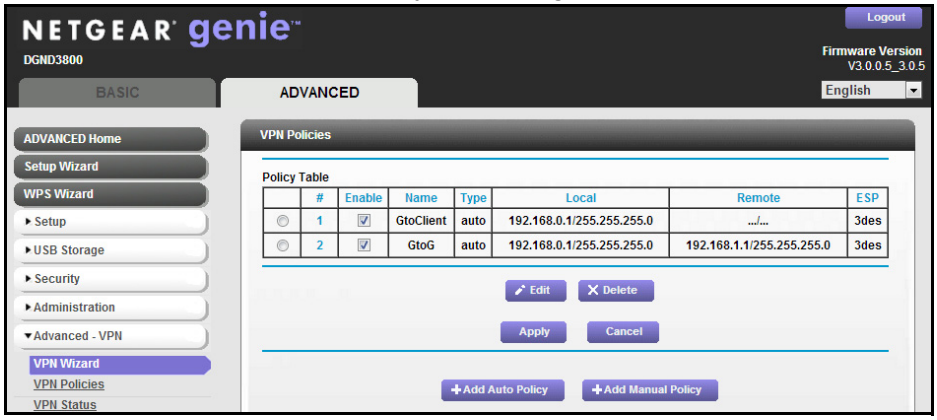
The VPN Wizard Summary screen displays:



To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link.

8. On the Summary screen click **Done**.

The VPN Policies screen displays, showing that the new tunnel is enabled.



9. Repeat these steps for the gateway on LAN B, and pay special attention to the following network settings:
   - WAN IP of the remote VPN gateway (for example, 14.15.16.17)
   - LAN IP settings of the remote VPN gateway:
     - IP address (for example, 192.168.0.1)
     - Subnet mask (for example, 255.255.255.0)
     - Pre-shared key (for example, 12345678)

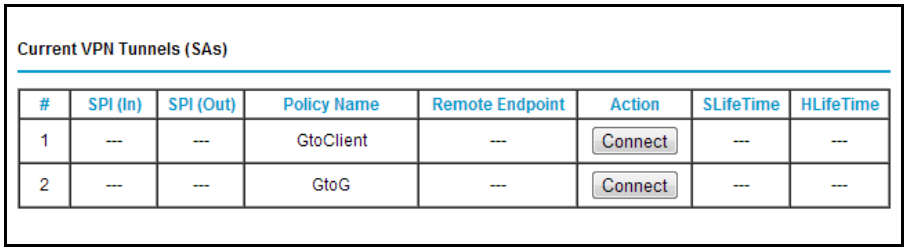
Activate a VPN Tunnel

To activate a VPN tunnel, you can use the VPN Status screen or start using the tunnel.

➢ **To use the VPN Status screen to activate a VPN tunnel:**

1. Select **ADVANCED > Advanced - VPN > VPN Status**.
2. Click **VPN Status**.

   The Current VPN Tunnels (SAs) screen displays.



3. Click **Connect** for the VPN tunnel that you want to activate.

➢ **To activate a VPN tunnel by using it:**

Use a web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

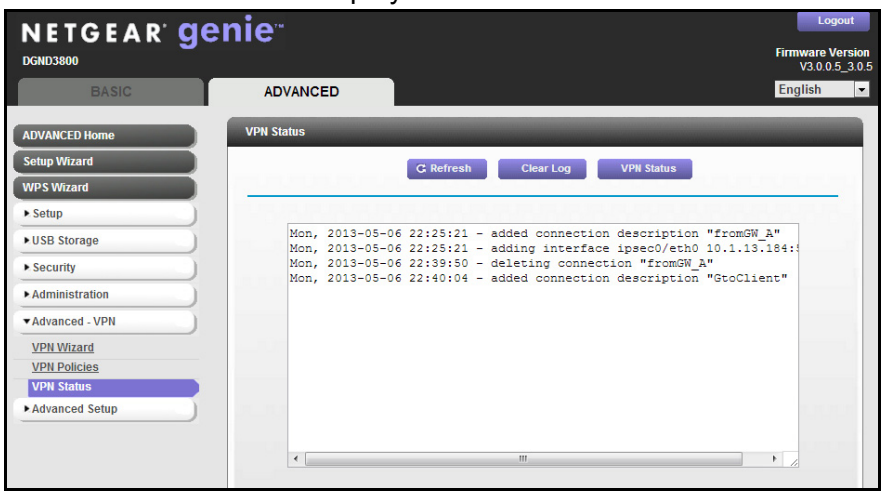
View or Change the Status of a VPN Tunnel

The VPN Status screen displays the status.

➢ **To check the status of a VPN tunnel:**

1. Select **ADVANCED > Advanced - VPN > VPN Status**.

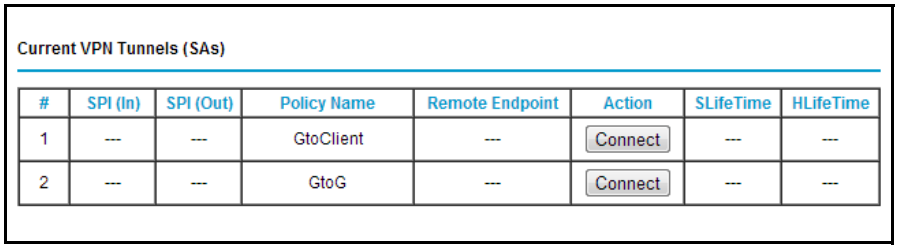
The VPN Status screen displays:



This log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

2. (Optional) Click **Refresh** to see the most recent entries.
3. (Optional) Click **Clear Log** to delete all log entries.
4. Click the **VPN Status** button.

The Current VPN Tunnels (SAs) screen displays.



This screen lists the following data for each active VPN tunnel.

- **SPI**. Each security association (SA) has a unique security parameter index (SPI) for traffic in each direction. For manual key exchange, the SPI is specified in the policy definition. For automatic key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**. The VPN policy associated with this SA.
- **Remote Endpoint**. The IP address on the remote VPN endpoint.
- **Action**. Either a Drop or a Connect button.
- **SLifeTime (Secs)**. The remaining soft lifetime for this SA in seconds. When the soft lifetime becomes 0 (zero), the SA is renegotiated.
- **HLifeTime (Secs)**. The remaining hard lifetime for this SA in seconds. When the hard lifetime becomes 0 (zero), the SA is terminated. (It is reestablished if necessary.)

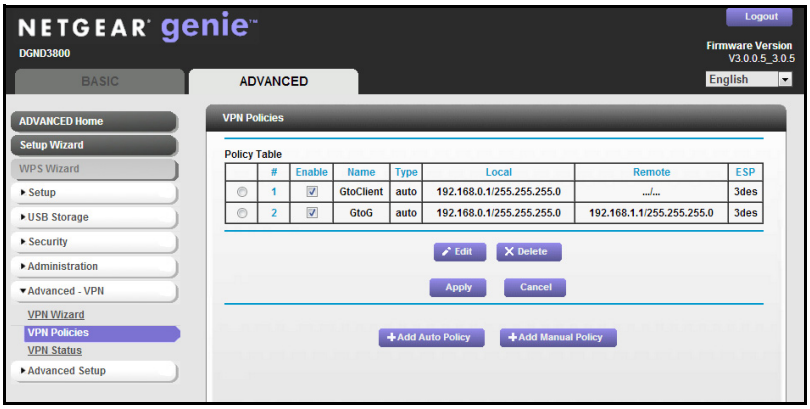
Deactivate a VPN Tunnel

Sometimes a VPN tunnel has to be deactivated for testing purposes. You can deactivate a VPN tunnel from two places:

- Policy table on VPN Policies screen
- VPN Status screen

➢ **To use the Policy Table to deactivate a VPN tunnel:**

1. Select **ADVANCED > Advanced - VPN > VPN Policies**.



2. In the Policy Table, clear the **Enable** check box for the VPN tunnel that you want to deactivate.
3. Click **Apply**.

To reactivate the tunnel, select the **Enable** check box and click **Apply**.

➢ **To use the VPN Status Screen to deactivate a VPN tunnel:**

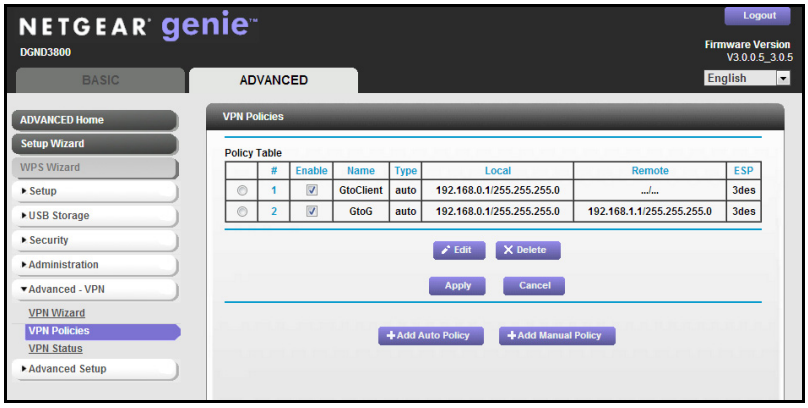
1. Select **ADVANCED > Advanced - VPN > VPN Status**.
2. Click **VPN Status**.

   The Current VPN Tunnels (SAs) screen displays.
3. Click **Drop** for the VPN tunnel that you want to deactivate.

Delete a VPN Tunnel

➢ **To delete VPN tunnel:**

1. Select **ADVANCED > Advanced - VPN > VPN Policies**.



2. Select the radio button for the VPN tunnel.
3. Click **Delete**.

Auto Policy Example

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end have to match to the inbound VPN settings on other end, and vice versa.

Auto policy creates a typical automated Internet Key Exchange (IKE) setup. Auto policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.

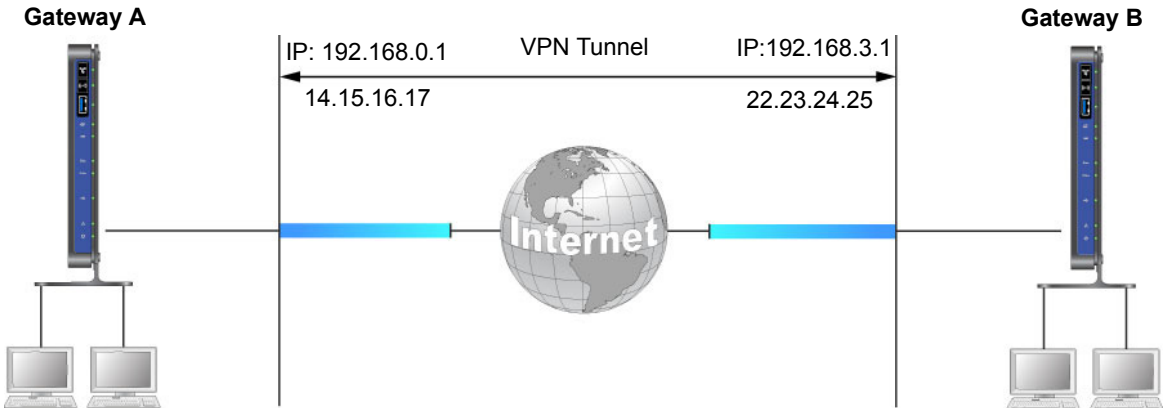


Figure 19. Example of an Auto policy for a gateway-to-gateway tunnel

Add or Edit a VPN Auto Policy

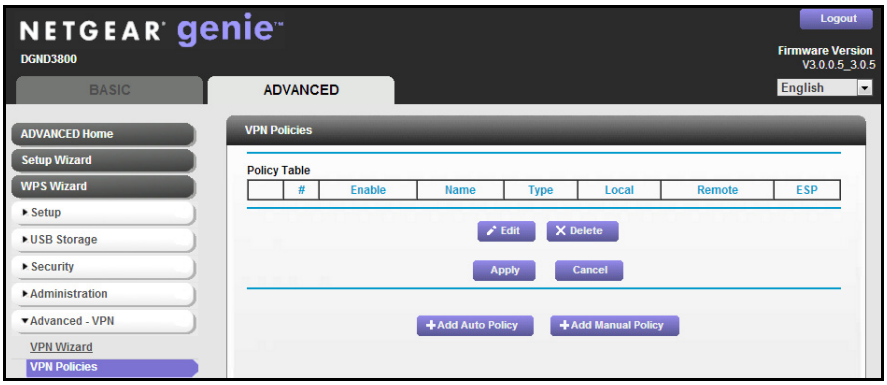
An Auto VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPSec SA (security association). Because of this negotiation, not all of the

settings on this VPN gateway have to match the settings on the remote VPN endpoint. Where settings have to match, this requirement is indicated.

➢ **To add an Auto policy:**

1. Set the LAN IPs on each gateway to different subnets and configure each correctly for the Internet.
2. Select **ADVANCED > Advanced - VPN > VPN Policies**.

   The VPN Policy screen displays:



3. Click the **Add Auto Policy** button.

   The VPN - Auto Policy screen displays:

Scroll to iew more ettings

4. Specify the general settings:
   - In the Policy Name field, enter a unique name.

This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

- From the Address Type list, select **Fully Qualified Domain Name**, **Dynamic IP Address** or **Fixed IP Address**.

  You can set up multiple remote dynamic IP policies, but only one policy can be enabled at a time.

- If you want to ensure that a connection is kept open, or, if that is not possible, it is quickly reestablished when disconnected, select the **IKE Keep Alive** check box and fill in the Ping IP Address field.

  The ping IP address has to be associated with the remote endpoint. Either the WAN or a LAN address can be used; a LAN address is preferable. This IP address is pinged to generate some traffic for the VPN tunnel.

5. Specify the Local LAN settings:
   - From the IP Address list, select **Subnet address**, **Single address**, or **Range address**.
   - Fill in the Single/Start IP Address field.
   - If you are specifying a range, fill in the Finish IP Address field.

     This range must be an address range used on your LAN. For a single IP address, do not fill in the Finish IP Address field.

   The remote VPN endpoint must have these IP addresses entered as its remote addresses.

6. Specify the Remote LAN settings.
   - From the IP Address list, select **Single PC -no Subnet**, **Single address**, **Range address**, or **Subnet address**.

     If there is no LAN (only a single computer) at the remote endpoint, select the **Single PC -no Subnet** option. The Single address option is typically used to access a server on the remote LAN.

   - If you want to specify a range, fill in the Finish IP Address field.

     This range must be an address range used on the remote LAN.

   - Fill in the Subnet Mask field.

   The remote VPN endpoint must have these IP addresses entered as its local addresses.

7. Specify the IKE settings:
   - From the Direction list, select either **Responder only** or **Initiator and Responder**.

     The modem router uses this setting to determine if the IKE policy matches the current traffic. With the Responder only setting, incoming connections are allowed and outgoing connections are blocked. With the Initiator and Responder setting, both incoming and outgoing connections are allowed.

   - Ensure that the remote VPN endpoint is set to use Main Mode.

- Select the Diffie-Hellman (DH) Group from the list.

  The Diffie-Hellman algorithm is used when keys are exchanged. The DH Group setting determines the bit size used in the exchange. This value needs to match the value used on the remote VPN gateway.

- Select the local identity type.

  Select an option to match the Remote Identity Type setting on the remote VPN endpoint.

  - **WAN IP Address**. Your Internet IP address.
  - **Fully Qualified Domain Name**. Your domain name.
  - **Fully Qualified User Name**. Your name, email address, or other ID.

- Select the remote identity type.

  Select the option that matches the Local Identity Type setting on the remote VPN endpoint.

  - **IP Address**. The Internet IP address of the remote VPN endpoint.
  - **Fully Qualified Domain Name**. The domain name of the remote VPN endpoint.
  - **Fully Qualified User Name**. The name, email address, or other ID of the remote VPN endpoint.

8. Specify the following parameters:
   - Select the encryption algorithm.

     This is the encryption algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. DES and 3DES are supported.

     - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
     - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

   - Select the authentication algorithm.

     This is the authentication algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode.

     - **MD5**. 128 bits, faster but less secure.
     - **SHA-1**. 160 bits, slower but more secure. This is the default.

   - Enter the pre-shared key.

     The key has to be entered both here and on the remote VPN gateway.

   - Enter the SA life time value.

This value is the time interval before the SA (security association) expires. (It is automatically reestablished as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA life time. This setting applies to both IKE and IPSec SAs.

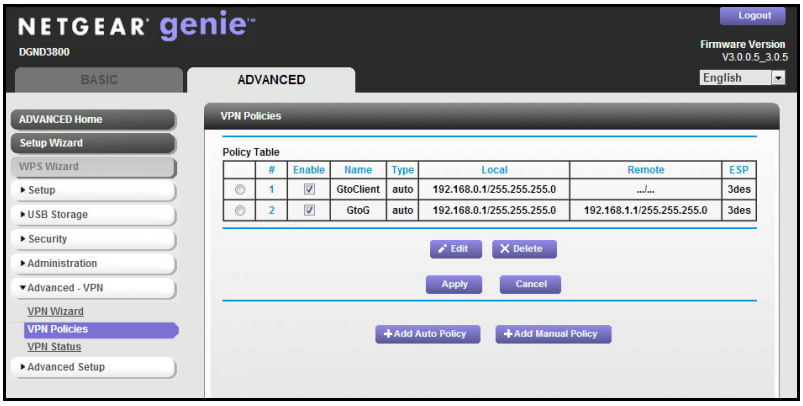
- If you want enhanced security, select the **Enable IPSec PFS (Perfect Forward Secrecy)** check box.

  If this check box is selected, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

  This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you might have to specify the key group used. For this device, the key group is the same as the DH Group setting in the IKE section.

9. Click **Apply**.

   The VPN Policies screen displays:



10. Repeat these steps for the gateway on LAN B.

    Pay special attention to the following network settings:

    - General, Remote Address Data (for example, 14.15.16.17)
    - Remote LAN, Start IP Address
      - IP Address (for example, 192.168.0.1)
      - Subnet Mask (for example, 255.255.255.0)
      - Pre-shared Key (for example, 12345678)

11. To activate the VPN tunnel, start using it, or use the VPN Status screen (select the tunnel and click **Connect**).

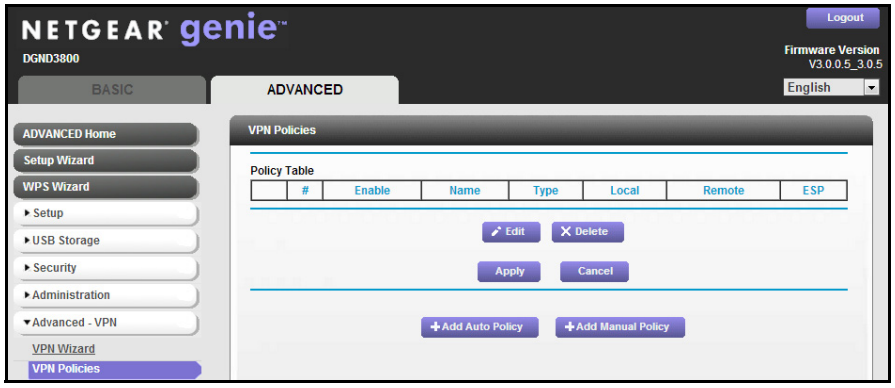
Add or Edit a Manual VPN Policy

A manual VPN policy requires all settings for the VPN tunnel to be manually entered at each end (both VPN endpoints).

➤ **To add or edit a manual policy:**

1. Select **ADVANCED > Advanced - VPN > VPN Policies**.

   The VPN Policies screen displays:



2. Click the **Add Manual Policy** button.

   The VPN - Manual Policy screen displays:

Scroll to view more setings

3. Specify the general settings:

   - In the Policy Name field, enter a unique name.

     This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

   - From the Address Type list, select **Fully Qualified Domain Name**, or select **Fixed IP Address**.

- Enter the domain name or Fixed IP address in the Address Data field.

You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time.

4. Specify the Local LAN settings:
   - From the IP Address list, select **Subnet address**, **Single address**, or **Range address**.
   - Fill in the Single/Start IP Address field.
   - If you are specifying a range, fill in the Finish IP Address field.

     This range must be an address range used on your LAN. For a single IP address, do not fill in the Finish IP Address field.

   The remote VPN endpoint must have these IP addresses entered as its remote addresses.
5. Specify the Remote LAN settings.
   - From the IP Address list, select **Single PC -no Subnet**, **Single address**, **Range address**, or **Subnet address**.

     If there is no LAN (only a single computer) at the remote endpoint, select the **Single PC -no Subnet** option. The Single address option is typically used to access a server on the remote LAN.
   - If you want to specify a range, fill in the Finish IP Address field.

     This range must be an address range used on the remote LAN.
   - Fill in the Subnet Mask field.

   The remote VPN endpoint must have these IP addresses entered as its local addresses.
6. Specify the ESP (Encapsulating Security Payload) settings:

   ESP provides security for the payload (data) sent through the VPN tunnel.
   - In the SPI field, enter the required security policy indexes (SPIs).

     Each policy has to have unique SPIs. These settings need to match the remote VPN endpoint. The **in** setting here has to match the **out** setting on the remote VPN endpoint, and the **out** setting here has to match the **in** setting on the remote VPN endpoint.
   - From the Encryption list, select **DES** or **3DES**, and fill in the Key field.

     For 3DES, the keys should be 24 ASCII characters, and for DES, the keys should be 8 ASCII characters.
     - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
     - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

- From the Authentication list, select **MD5** or **SHA-1**, and fill in the Key field.

Troubleshooting

10

This chapter provides information to help you diagnose and solve problems you might have with your modem router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Troubleshoot with the LEDs*
- *Cannot Log In to the Modem Router*
- *Troubleshoot the Internet Connection*
- *TCP/IP Network Not Responding*
- *Cannot Log In*
- *Changes Not Saved*
- *Incorrect Date or Time*

Troubleshoot with the LEDs

When you turn on the power, the Power, LAN, and DSL LEDs should light as described here. If they do not, refer to the sections that follow for help.

1. When power is first applied, the Power LED lights.
2. After approximately 10 seconds, the LAN and DSL LEDs light as follows:
   a. The LAN port LEDs light for any local ports that are connected.
   b. The 2.4 GHz and 5 GHz Wireless LEDs light.
   c. The DSL link LED lights when there is a link through the ADSL phone lines.
   d. The Internet LED lights to indicate a connection to the ISP.

Power LED Is Off

If the Power and other LEDs are off when your modem router is turned on:

- Check that the power cord is correctly connected to your modem router and the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you could have a hardware problem and should contact NETGEAR technical support.

Power LED Is Red

When the modem router is turned on, it performs a power-on self-test, during which time the Power LED turns red. If the Power LED does not turn green within a minute or so or if it turns red at any other time during normal operation, there is a fault within the modem router.

If the Power LED turns red to indicate a modem router fault, turn the power off and on to see if the modem router recovers. If the Power LED is still red 1 minute after power-up:

- Turn the power off and on one more time to see if the modem router recovers.
- Clear the modem router's configuration to factory defaults as explained in *Factory Settings* on page 149. This sets the modem router's IP address to 192.168.0.1.

If the error persists, you could have a hardware problem and should contact NETGEAR technical support.

LAN LED Is Off

If the LAN LED for a port does not light when you connect a device, check the following:

- The Ethernet cable connections are secure at the modem router and at the hub or device.
- The power is turned on to the connected hub or device.

- You are using the correct cable.

Wireless LEDs Are Off

If the 2.4 GHz and 5 GHz Wireless LEDs do not light, the radios might be turned off. Press the **Wireless On/Off** button on the front panel to turn the radios back on.

DSL or Internet LED Is Off

If the DSL or Internet LED does not light, check to make sure that you are using the correct cable. When connecting the ADSL or Ethernet WAN port, use the cables that were supplied with the modem router. If the DSL or Internet LED is still off, this could mean that there is no ADSL or fiber/cable modem service or the cable connected to the ADSL or Ethernet WAN port is bad.

See also *DSL LED Is Off* on page 142.

Cannot Log In to the Modem Router

If you are unable to log in to the modem router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the modem router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the modem router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem router, and reboot your computer.
- If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults. This sets the modem router's IP address to 192.168.0.1. This procedure is explained in *Factory Settings* on page 149.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

Troubleshoot the Internet Connection

If your modem router is unable to access the Internet, check the ADSL connection, then the WAN TCP/IP connection.

ADSL Link

First determine whether you have an ADSL link with the service provider. The state of this connection is indicated by the DSL LED.

DSL LED Is Green or Blinking Green

You have a good ADSL connection. The service provider has connected your line correctly, and your wiring is correct.

DSL LED Is Blinking Amber

Your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the DSL LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone. For more information, see *ADSL Microfilters* on page 13. If you connect the microfilters correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID) and the signal is okay, you might have poor-quality wiring in your house.

DSL LED Is Off

First disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It could be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device could not connect to the Internet. Verify the following:

- Check that your login credentials are correct. For more information, see *Log In to the N600 Modem Router* on page 18.
- Check that the information you entered on the Basic Settings screen is correct. For more information, see *Manual Setup (Basic Settings)* on page 22.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Find out if the ISP is having a problem. If it is, wait until that problem is cleared up and try again.

Obtaining an Internet IP Address

If your modem router is unable to access the Internet, and your Internet LED is green, see if the modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router requests an IP address from the ISP. You can determine whether the request was successful using the browser interface.

➢ **To check the Internet IP address from the browser interface:**

1. Launch your browser, and select an external site such as *www.netgear.com*.
2. Access the main menu of the modem router's configuration at http://192.168.0.1.
3. Click the **ADVANCED** tab and check that an IP address is shown for the WAN port.

   If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your modem router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrectly set. For more information, see the following section, *Troubleshoot PPPoE or PPPoA* .
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the modem router's MAC address.
  - Configure your modem router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

Troubleshoot PPPoE or PPPoA

➢ **To troubleshoot a PPPoE or PPPoA connection:**

1. Select **ADVANCED > Administration > Router Status**.
2. Click the **Connection Status** button.
3. Check t o see if your PPPoE or PPPoA connection is up and working.
4. If any of the fields on the Connection Status screen indicates Failed, you can attempt to reconnect by clicking **Connect**.

   The modem router continues to attempt to connect indefinitely.
5. If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the modem router does not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshoot Internet Browsing

If your modem router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address when you set up the modem router, reboot your computer, and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer might not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address.

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Modem Router

You can ping the modem router from your computer to verify that the LAN path to your modem router is set up correctly.

➢ **To ping the modem router from a computer running Windows 95 or later:**

1. From the Windows taskbar, click the **Start** button, and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the modem router, as in this example:

   ping 192.168.0.1

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections

     Make sure that the LAN port LED is lit. If the LED is off, follow the instructions in *LAN LED Is Off* on page 140.

   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
     - Verify that the IP address for your modem router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your computer to a remote device. In the Windows Run screen, type:

```
ping -n 10 IP address
```

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as described in *Test the LAN Path to Your Modem Router* on page 145 display. If you do not receive replies:

- Check that your computer has the IP address of your modem router listed as the default modem router. If the IP configuration of your computer is assigned by DHCP, this

information is not visible in your computer's Network Control Panel. Verify that the IP address of the modem router is listed as the default router.

- Check that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Setup screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single computer connected to that modem. In this case, configure your modem router to clone or spoof the MAC address from the authorized computer.

Cannot Log In

If you cannot log in to the modem router from a computer on your local network, check the following:

- The router is plugged in and it is on.
- You are using the correct login information. The login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you cannot connect wirelessly, try an Ethernet connection and view the router wireless settings and set up your wireless computer with corresponding wireless settings.
- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router. The LAN LED for the port you are using on the router should light up to show your connection.
- Your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range 192.168.0.2 to 192.168.0.254.
- If the computer IP address is 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address when the computer cannot reach a DHCP server. The autogenerated addresses are in the range 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. For more information, see *Factory Settings* on page 149. This sets the router's IP address to 192.168.0.1.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try closing the browser and relaunching it.

Changes Not Saved

If the modem router does not save the changes you make in the modem router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Incorrect Date or Time

The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2003. This means the modem router has not yet reached a network time server. Check that your Internet access is configured correctly. If you have just finished setting up the modem router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. The modem router has an automatic daylight savings time setting.

➢ **To change the modem router setting for daylight savings time:**

1. Select **ADVANCED > Security > Schedule**.
2. Select the **Automatically adjust for daylight savings time** check box.
3. Click **Apply**.

   Your change is saved.

Supplemental Information

This appendix includes the factory default settings and technical specifications for the modem router.

This appendix contains the following sections:

- *Factory Settings*
- *Specifications*

Factory Settings

You can return the modem router to its factory settings. On the bottom of the modem router, use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button for at least 7 seconds. The modem router returns to the factory settings shown in the following table.

Table 4. Factory default settings

Feature		Default Behavior
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1492
	Port speed	AutoSensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	GMT for WW except GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table 4. Factory default settings (continued)

Feature		Default Behavior
Wireless	Wireless communication	Enabled
	SSID name	Can be found on the label on the bottom of the unit.
	Security	Can be found on the label on the bottom of the unit.
	Broadcast SSID	Enabled
	Country/region	United States (in North America; otherwise, varies by region)
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Pre-shared Key
	Wireless Card Access List	All wireless stations allowed

Specifications

Table 5. DGND3800 modem router specifications

Specification	Description
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input
	UK, Australia: 240V, 50 Hz, input
	Europe: 230V, 50 Hz, input
	All regions (output): 12V @ 1A output
Physical	Dimensions: 6.80 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm)
	Weight: 0.61 lbs (0.275 kg)
Environmental	Operating temperature: 0° to 40° C (32º to 104º F)
	Operating humidity: 10% to 90% relative humidity, noncondensing
	Storage temperature: –20° to 70° C (–4º to 158º F)
	Storage humidity: 5 to 95% relative humidity, noncondensing
Regulatory compliance	FCC Part 15 Class B, VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface specifications	LAN: 10BASE-T or 100BASE-Tx, RJ-45 (Gigabit Ethernet) WAN: ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT RJ-45 WAN port (Gigabit Ethernet)

VPN Configuration

B

Case study on how to set up a VPN

The DGND3800B can terminate up to five VPNs. This appendix is a case study on how to configure a secure IPSec VPN tunnel from your modem router to an FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

The following topics are discussed:

- *Configuration Profile*
- *Modem Router with FQDN to Gateway B*
- *Configuration Summary (Telecommuter Example)*
- *Set Up Client-to-Gateway VPN (Telecommuter Example)*
- *Monitor the VPN Tunnel (Telecommuter Example)*

Configuration Profile

The configuration in this appendix follows the addressing and configuration mechanics defined by the VPN Consortium. Gather necessary information before you begin configuration. Verify that the firmware is up to date, and that you have all the addresses and parameters to be set on both sides. Check that there are no firewall restrictions.

Table 6. Wireless modem router to Gateway B profile summary

VPN Consortium Scenario		Scenario 1 (Identity Using Preshared Secrets)
Type of VPN		LAN-to-LAN or gateway-to-gateway (not client-to-gateway)
Security scheme:		IKE with pre-shared secret/key (not certificate based)
IP addressing:		
	Gateway A	Static IP address
	Gateway B	Static IP address

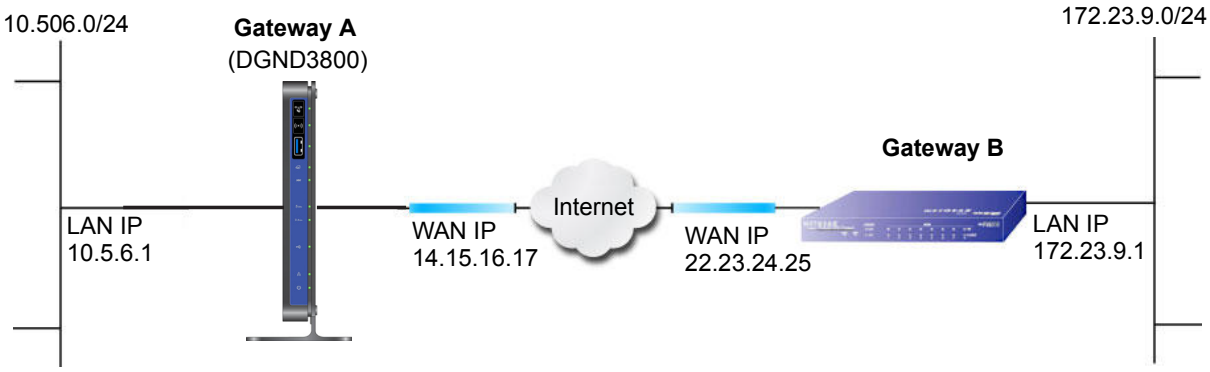


Figure 20. VPNC example, network interface addressing

Step-by-Step Configuration

➢ **To configure a VPN tunnel:**

1. Use the VPN Wizard to configure Gateway A (DGND3800B) for a gateway-to-gateway tunnel (see *Add a Gateway-to-Gateway VPN Tunnel* on page 125), being certain to use appropriate network addresses for the environment.

   The LAN addresses used in this example are as follows:

Unit	WAN IP	LAN IP	LAN Subnet Mask
DGND3800B	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.13.24.25	172.23.9.1	255.255.255.0

   a. For the connection name, enter **toGW_B**.

b. For the remote WAN's IP address, enter **22.23.24.25**.

c. Enter the following:

- IP Address. **172.23.9.1**
- Subnet Mask. **255.255.255.0**

d. In the Summary screen, click **Done**.

2. Use the VPN Wizard to configure the Gateway B for a gateway-to-gateway tunnel (see *Add a Gateway-to-Gateway VPN Tunnel* on page 125), being certain to use appropriate network addresses for the environment.

a. For the connection name, enter **toGW_A**.

b. For the remote WAN's IP address, enter **14.15.16.17**.

c. Enter the following:

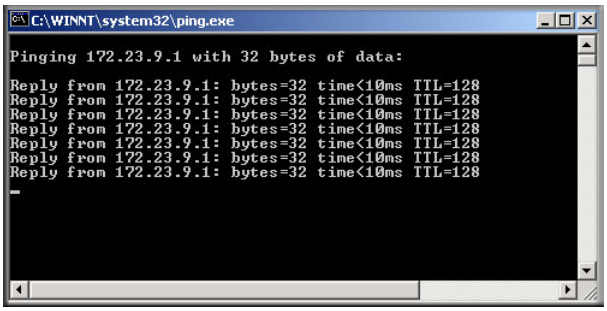
- IP Address. **10.5.6.1**
- Subnet Mask. **255.255.255.0**

d. In the Summary screen, click **Done**.

3. Test the VPN tunnel by pinging the remote network from a computer attached to Gateway A (modem router).

a. Open the command prompt (select **Start > Run > cmd**).

b. Type `ping 172.23.9`.



If the pings fail the first time, try the pings a second time.

Modem Router with FQDN to Gateway B

This section is a case study on how to configure a VPN tunnel from your modem router to a gateway using a fully qualified domain name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (visit *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

Configuration Profile

The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration.

Verify that the firmware is up to date, and that you have all the addresses and parameters to be set on both sides. Check that there are no firewall restrictions.

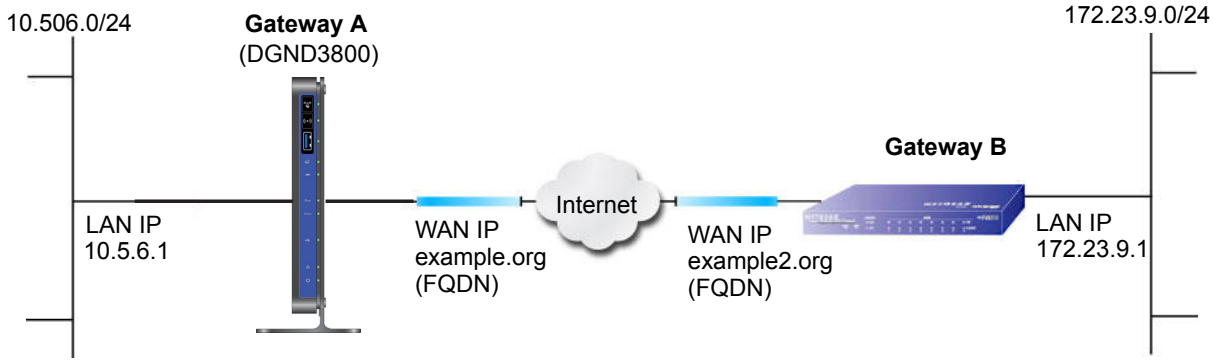


Figure 21. VPNC example, network interface addressing

Table 7. Wireless modem router with FQDN to Gateway B profile summary

VPN Consortium Scenario		Scenario 1
Type of VPN		LAN-to-LAN or gateway-to-gateway (not client-to-gateway)
Security scheme:		IKE with pre-shared secret/key (not certificate based)
IP addressing:		
	Gateway A	Fully qualified domain name (FQDN)
	Gateway B	FQDN

Use a Fully Qualified Domain Name (FQDN)

Many ISPs provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time, which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as email addresses, host names, and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a third-party service instead of a permanent and unchanging IP address to establish bidirectional VPN connectivity.

To use DDNS, you have to register with a DDNS service provider. Some DDNS service providers include:

- **DynDNS**. www.dyndns.org
- **TZO.com**. netgear.tzo.com
- **ngDDNS**. ngddns.iego.net

In this example, Gateway A is configured using a sample FQDN provided by a DDNS service provider. In this case the host name dgnd3800.dyndns.org for Gateway A was provided using the DynDNS service. Gateway B uses the DDNS service provider when establishing a VPN tunnel.

To establish VPN connectivity, Gateway A has to be configured to use Dynamic DNS, and Gateway B has to be configured to use a DNS host name provided by a DDNS service provider to find Gateway A. Again, the following step-by-step procedures assume that you have already registered with a DDNS service provider and have the configuration information necessary to set up the gateways.

Step-by-Step Configuration

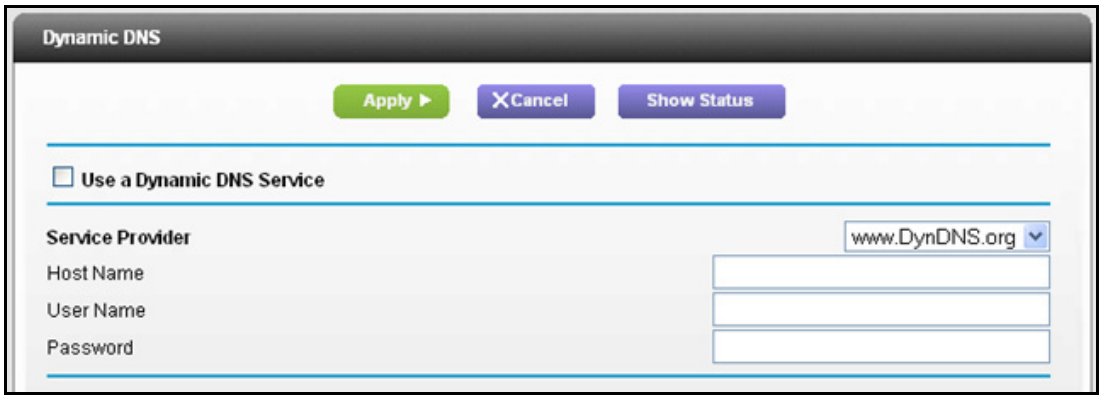
➢ **To configure a VPN tunnel:**

1. Log in to Gateway A (your modem router) as described in *Use NETGEAR genie after Installation* on page 21.

   This example assumes that you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. On Gateway A, configure the Dynamic DNS settings.

   a. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

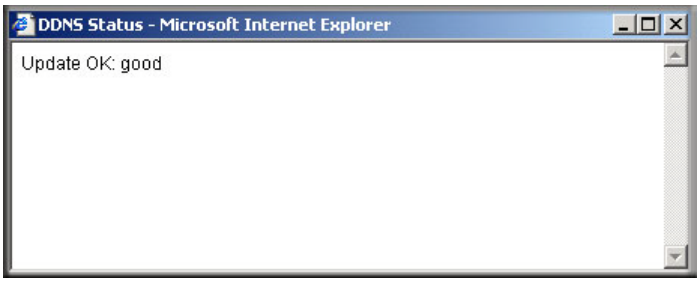


   b. Fill in the fields with account and host name settings.
      - Select the **Use a Dynamic DNS Service** check box.
      - In the Host Name field, type **dgnd3800.dyndns.org**.
      - In the User Name field, enter the account user name.
      - In the Password field, enter the account password.

   c. Click **Apply**.

   d. Click **Show Status**.

      The resulting screen should show Update OK: good:

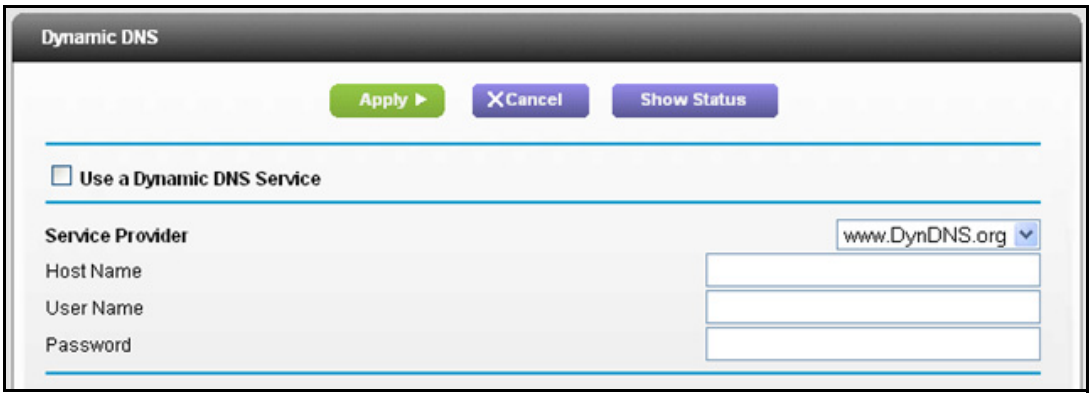


3. On Gateway B, configure the Dynamic DNS settings.

   Assume a correctly configured DynDNS account.

   a. Select **ADVACNED > Advanced Setup > Dynamic DNS**.

      The Dynamic DNS screen displays:



   b. Select the **Use a Dynamic DNS Service** check box.

   c. Select **www.DynDNS.org** from the Service Provider drop-down list.

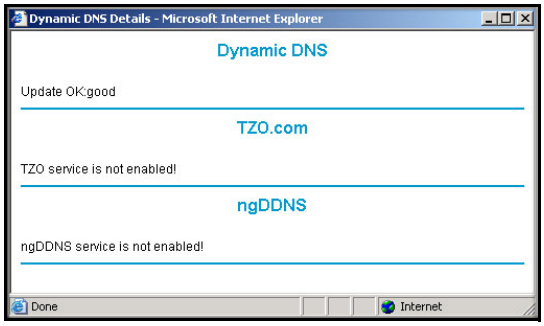
   d. Fill in the fields with the account and host name settings.

      - In the Host Name field, enter **fvl328.dyndns.org**.
      - In the User Name field, enter the account user name.
      - In the Password field, enter the account password.

   e. Click **Apply.**

   f. Click **Show Status**.

      The resulting screen should show Update OK: good:



4. Configure the modem router as in the gateway-to-gateway procedures using the VPN Wizard (see *Add a Gateway-to-Gateway VPN Tunnel* on page 125), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:

Table 8.

Device	LAN IP Address	LAN Subnet Mask
DGND3800B	10.5.6.1	255.255.255.0
FVL328	172.23.6.1	255.255.255.0

a. For the connection name, enter **toFVL328**.

b. For the remote WAN's IP address, enter **fvl328.dyndns.org**.

c. Enter the following:

- IP Address. **172.23.9.1**
- Subnet Mask. **255.255.255.0**

5. Configure the FVL328 as in the gateway-to-gateway procedures for the VPN Wizard (see *Add a Gateway-to-Gateway VPN Tunnel* on page 125), being certain to use appropriate network addresses for the environment.

a. For the connection name, enter **toDGND3800**.

b. For the remote WAN's IP address, enter **dgnd3800.dyndns.org**.

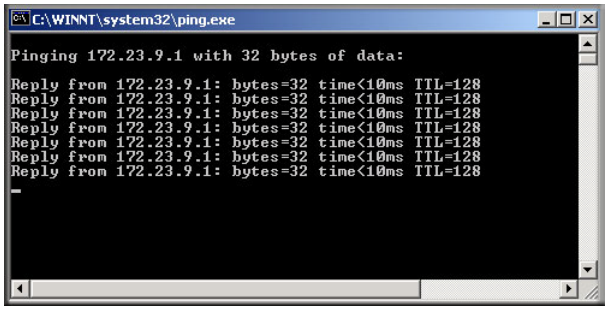
c. Enter the following:

- IP Address. **10.5.6.1**
- Subnet Mask. **255.255.255.0**

6. Test the VPN tunnel by pinging the remote network from a computer attached to the modem router.

a. Open the command prompt (select **Start > Run > cmd**).

b. Type `ping 172.23.9.1`.



If the pings fail the first time, try the pings a second time.

Configuration Summary (Telecommuter Example)

The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration.

Verify that the firmware is up to date, and make sure you have all the addresses and parameters to be set on both sides. Assure that there are no firewall restrictions.

Table 9. Configuration summary (telecommuter example)

VPN Consortium Scenario		Scenario 1
Type of VPN:		Client-to-gateway, with client behind NAT router
Security scheme:		IKE with pre-shared secret/key (not certificate based)
IP addressing:		
	Gateway	Fully qualified domain name (FQDN)
	Client	Dynamic

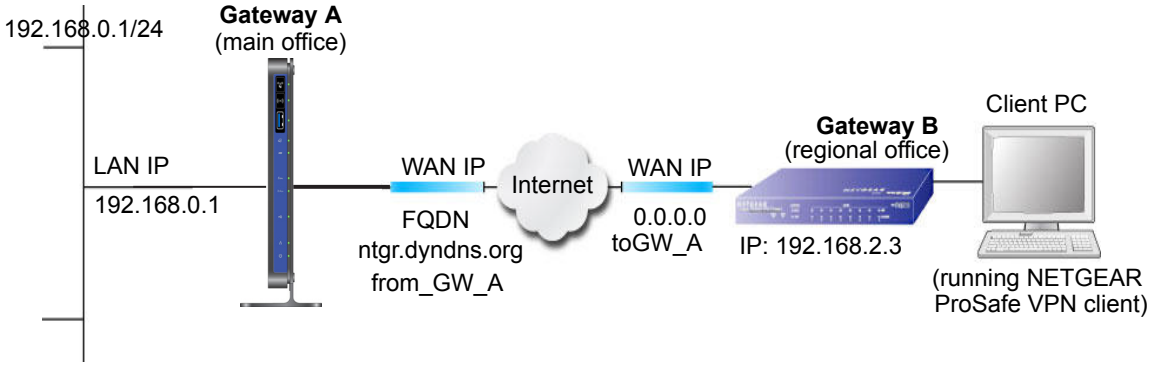


Figure 22. Telecommuter example

Set Up Client-to-Gateway VPN (Telecommuter Example)

Setting up a VPN between a remote computer running the NETGEAR ProSafe VPN client and a network gateway involves two steps, described in the following sections:

- *Configure Gateway A (VPN Router at Main Office)* on page 159.
- *Configure Gateway B (VPN Router at Regional Office)* on page 160 describes configuring the NETGEAR ProSafe VPN client endpoint.

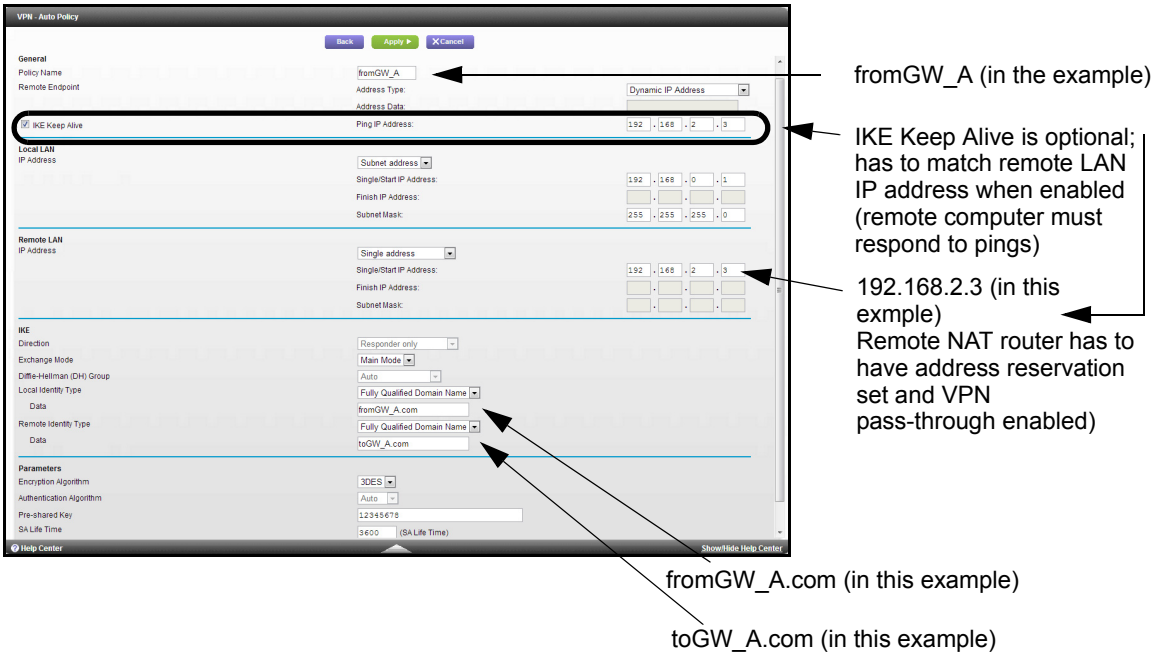
Configure Gateway A (VPN Router at Main Office)

➢ **To configure a VPN tunnel:**

1. Log in to the VPN router.
2. Select **ADVANCED > Advanced - VPN > VPN Policies**.
3. Click the **Add Auto Policy** button.

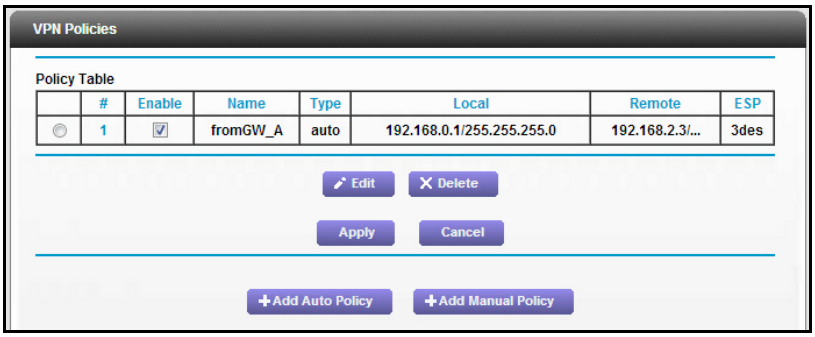
   The VPN - Auto Policy screen displays.

Enter the following information:



4. Click **Apply**.

   The VPN Policies screen displays.



To view or modify the tunnel settings, select the radio button next to the tunnel entry, and then click **Edit**.

Configure Gateway B (VPN Router at Regional Office)

This procedure assumes that the computer running the client has a dynamically assigned IP address.

The computer has to have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Visit the NETGEAR website (*www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN Client.

Note: Before installing the software, be sure to turn off any virus protection or firewall software you might be running on your computer.

➢ **To configure a VPN tunnel:**

1. Install the NETGEAR ProSafe VPN Client on the remote computer, and then reboot.
   a. You might need to insert your Windows CD to complete the installation.

      If you do not have a modem or dial-up adapter installed in your computer, you might see the warning message stating, “The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed.” Disregard this message.

   b. Install the IPSec component.

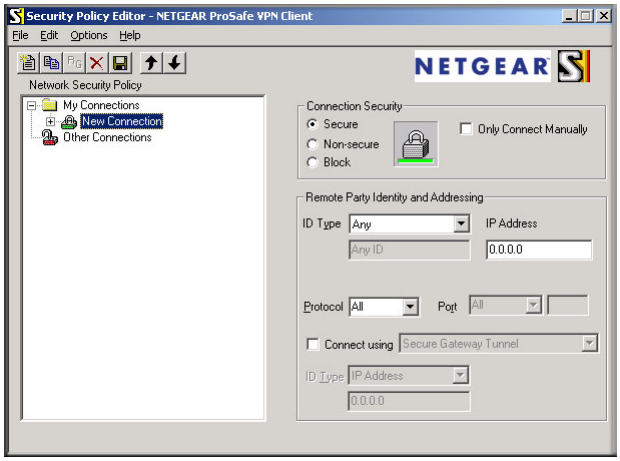
      You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

      The system should show the ProSafe icon ( ) in the system tray after you reboot.

   c. Double-click the system tray icon to open the Security Policy Editor.
2. Add a new connection.
   a. Run the NETGEAR ProSafe Security Policy Editor program, and create a VPN connection.
   b. From the Edit menu of the Security Policy Editor, select **Add > Connection**.

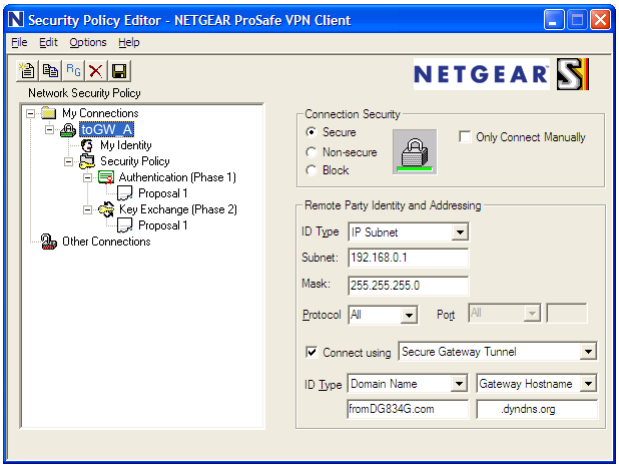
      A New Connection listing appears in the list of policies.

   c. Rename the new connection to match the connection name you entered in the VPN settings of Gateway A. Choose connection names that make sense to the people using and administering the VPN.



Note: *In this example, the connection name on the client side of the VPN tunnel is toGW_A. It does not have to match the VPN-client connection name used on the gateway side of the VPN tunnel because connection names do not affect how the VPN tunnel functions.*

d. In the Connection Security section, select **Secure**.



e. In the ID Type drop-down list, select **IP Subnet**.

f. In the Subnet field, type **192.168.0.1** as the network address of the modem router.

g. In the Mask field, enter **255.255.255.0** as the LAN subnet mask of the modem router.

h. In the Protocol drop-down list, select **All** to allow all traffic through the VPN tunnel.

i. Select the **Connect using Secure Gateway Tunnel** check box.

j. In the ID Type drop-down list, select **Domain Name**, and enter **fromGW_A.com**.

k. Select **Gateway Hostname** and enter **ntgr.dyndns.org**.

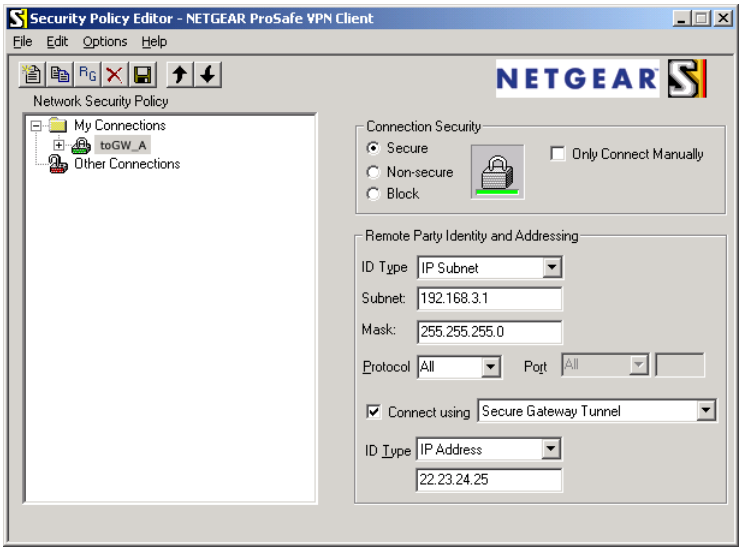
3. Configure the security policy in the modem router software.

a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the **+** symbol.

My Identity and Security Policy appear below the connection name.

b. Click **Security Policy**.

The Security Policy screen displays:

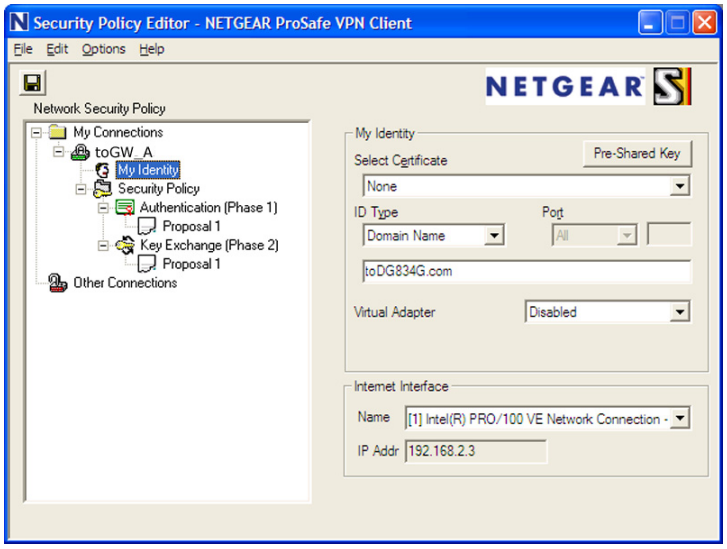


c. In the Select Phase 1 Negotiation Mode group, select the **Main Mode** radio button.

4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client computer. You have to provide the pre-shared key that you configured in the modem router and either a fixed IP address or a fixed virtual IP address of the VPN client computer.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, click **My Identity**.



b. In the Select Certificate list, select **None**.

c. In the ID Type list, select **Domain Name**, and enter **toGW_A.com**.

d. In the Virtual Adapter list, select **Disabled**.

e. In the Internet Interface section, in the Name list, select **Intel PRO/100VE Network Connection**; your Ethernet adapter might be different), and then in the IP Addr field, enter **192.168.2.3**.

f. Click the **Pre-Shared Key** button.

g. In the Pre-Shared Key screen, click **Enter Key**. Enter the modem router's pre-shared key and click **OK**.

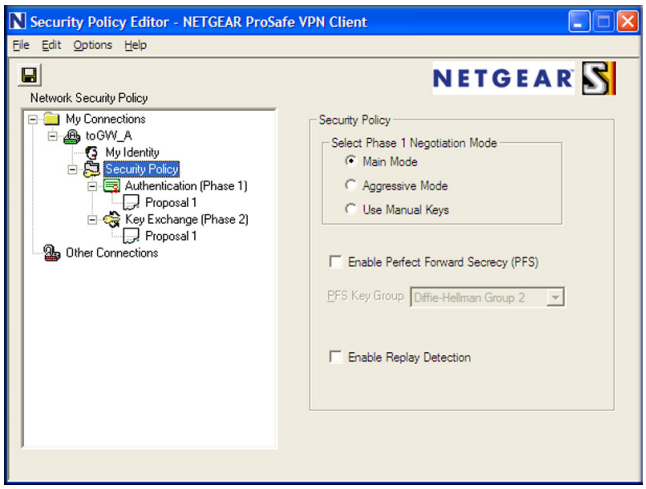
In this example, 12345678 is entered, though the screen shows asterisks. This field is case-sensitive.

5. Configure the VPN Client Authentication Proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the VPN router configuration.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double-clicking its name or clicking the **+** symbol.

b. Expand the Authentication subheading by double-clicking its name or clicking the **+** symbol. Then select **Proposal 1** below Authentication.



c. In the Authentication Method drop-down list, select **Pre-Shared Key**.

d. In the Encrypt Alg drop-down list, select the type of encryption. In this example, use **Triple DES**.

e. In the Hash Alg drop-down list, select **SHA-1**.

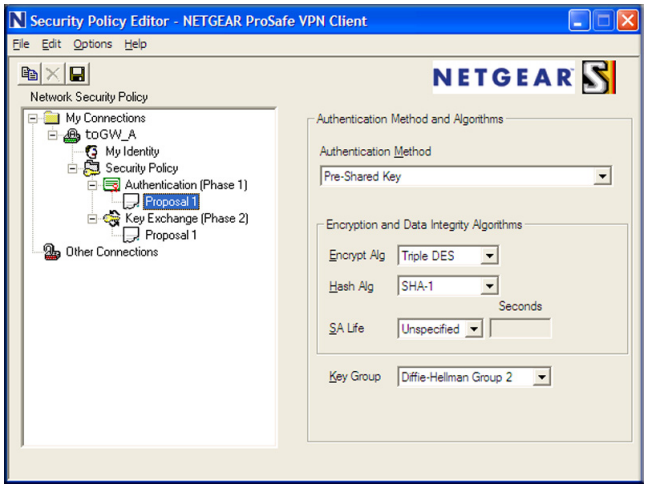
f. In the SA Life drop-down list, select **Unspecified**.

g. In the Key Group drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the VPN Client Key Exchange Proposal.

   In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the VPN router configuration.

   a. Expand the Key Exchange subheading by double-clicking its name or clicking the **+** symbol. Then select **Proposal 1** below Key Exchange.



   b. In the SA Life drop-down list, select **Unspecified**.

   c. In the Compression drop-down list, select **None**.

   d. Select the **Encapsulation Protocol (ESP)** check box.

   e. In the Encrypt Alg drop-down list, select the type of encryption. In this example, use **Triple DES**.

   f. In the Hash Alg drop-down list, select **SHA-1**.

   g. In the Encapsulation drop-down list, select **Tunnel**.

   h. Leave the **Authentication Protocol (AH)** check box cleared.

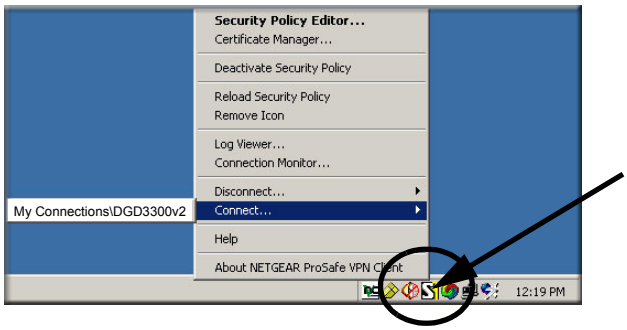
7. Save the VPN client settings.

   From the File menu at the top of the Security Policy Editor window, select **Save**.

   After you have configured and saved the VPN client information, your computer automatically opens the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

8. Check the VPN connection.

To check the VPN connection, you can initiate a request from the remote computer to the VPN router's network by using the Connect option in the modem router screen:



Right-click the system tray icon to open the pop-up menu.

Since the remote computer has a dynamically assigned WAN IP address, it has to initiate the request.

a. Right-click the system tray icon to open the pop-up menu.

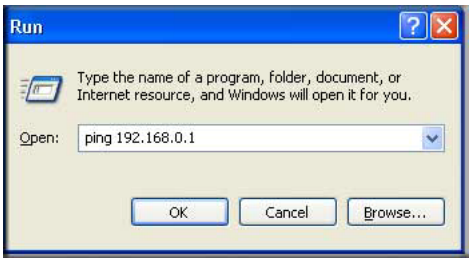
b. Select **Connect** to open the My Connections list.

c. Select **toDGND3800**.

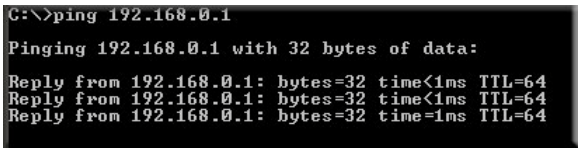
The modem router reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

➢ **To perform a ping test using this example, start from the remote computer:**

1. Establish an Internet connection from the computer.
2. On the Windows taskbar, click the **Start** button, and then select **Run**.
3. Type **`ping -t 192.168.0.1`**, and then click **OK**.



This causes a continuous ping to be sent to the VPN router. Within 2 minutes, the ping response should change from `timed out` to `reply`.



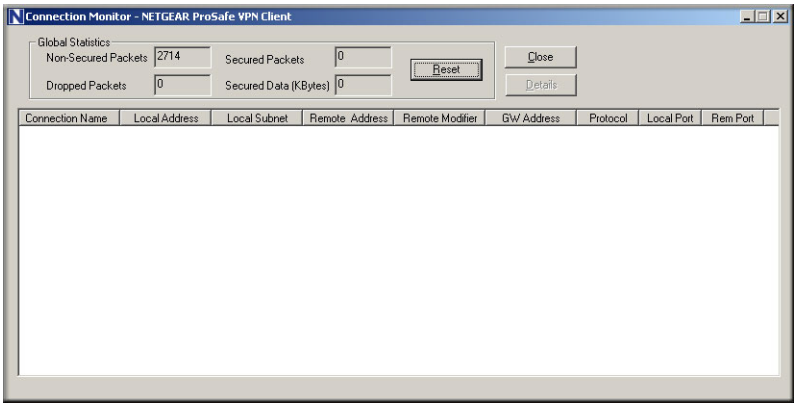
Once the connection is established, you can open the browser on the computer and enter the LAN IP address of the VPN router. After a short wait, you should see the login screen of the VPN router (unless another computer already has the VPN router management interface open).

Monitor the VPN Tunnel (Telecommuter Example)

To view information about the progress and status of the VPN client connection, open the Log Viewer. In Windows, click **Start**, and select **Programs > N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B > Log Viewer**.

Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

The Connection Monitor screen displays:



While the connection is being established, the connection name listed in this screen shows SA before the name of the connection. When the connection is successful, the SA changes to the yellow key symbol.

Note: While your computer is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you need to close the VPN connection to have normal Internet access.

Notification of Compliance

C

NETGEAR Dual Band - Wireless

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the CE marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

Intended for indoor use only in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA / Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce po-tential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utili-sation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Interference Reduction Table

The following table shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters